

クラウドコンピューティングのセキュリティについて

(平成30年度)

C I S S P 堀合 啓一

(Certified Information Systems Security Professional)

平成30年12月

公益財団法人 防衛基盤整備協会



発刊にあたって

情報処理における効率性の追求やセキュリティ水準の向上などの観点から、クラウドコンピューティングの活用が広がっています。総務省は「自治体クラウドサービスポータルサイト」¹などを通じて、クラウドサービスの利用を推進してきました。また、セキュリティの確保に必要なガイドラインとして「クラウドサービス提供における情報セキュリティ対策ガイドライン」²などを策定し公開しています。また、政府は2018年6月に「クラウドサービスの利用に係る基本方針」³を決定し、この中でコスト削減や柔軟なリソースの増減等への対応の観点から行政情報システムの第一候補としてクラウドサービスの利用を掲げています（クラウド・バイ・デフォルト）。

一方、米国政府は、2010年に「クラウド・ファースト」ポリシーを策定し、政府機関の情報処理システムをクラウドコンピューティングへ積極的に移行してきました。クラウドの活用の際に、どのようにしてセキュリティを担保するかが問題となりますが、米国では情報セキュリティに焦点を当てた NIST の SP-800 シリーズなどの刊行物が充実しています。さらに米国共通役務庁(GSA)が中心となって FedRAMP と呼ばれるフレームワークを策定し、アセスメントを経て認定を取得したサービスのリストを公開しています。クラウドサービスの利用者は、取り扱う情報の格付けなどのニーズに応じて、リストの中から既存のサービスを選択して利用することができ、利用開始までの時間やコストを削減できる仕組みとなっています。

さらに、政府機関の中でも、より厳しいセキュリティを求められる米国国防総省では、FedRAMP を基に独自の要件を追加した CC SRG(Cloud Computing Security Requirement Guide)を策定しています。また、米国の Amazon が提供しているクラウドサービス AWS の中に、米国政府機関の秘の情報を扱うことが可能な Secret Zone のサービスを2017年11月に開始する旨のアナウンスがあり⁴、さらにクラウドコンピューティングの利用範囲が拡大する可能性があります。

このような背景の下で、本調査研究は、我が国よりもクラウドコンピューティングの利用が先行している米国 DoD のクラウドコンピューティングのセキュリティガイドラインである CC SRG の翻訳を試みたものであります。

今後、我が国においてもクラウドコンピューティングの環境で、保護すべき情報などを扱う場合のセキュリティに関するガイドライン等として参考になれば幸甚であります。

平成30年12月

公益財団法人 防衛基盤整備協会
理事長 鎌田 昭良

¹ http://www.soumu.go.jp/main_sosiki/jichi_gyousei/c-gyousei/lg-cloud/

² http://www.soumu.go.jp/main_content/000283647.pdf

³ https://cio.go.jp/sites/default/files/uploads/documents/cloud_%20policy.pdf

⁴ <https://aws.amazon.com/jp/blogs/publicsector/announcing-the-new-aws-secret-region/>

クラウドコンピューティング セキュリティ要求ガイド

DEPARTMENT OF DEFENSE
CLOUD COMPUTING SECURITY REQUIREMENTS GUIDE

Version 1, Release 3 6 March, 2017

文書の翻訳及び開示にあたっては事前に DISA (Defense Information Systems Agency) から承認を得ております。

本文書は、原点に沿ってできるだけ忠実に翻訳するよう努めていますが、完全に正確であることを保証するものではありません。

当協会は、本文書に記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。

DEPARTMENT OF DEFENSE

CLOUD COMPUTING SECURITY REQUIREMENTS GUIDE

クラウドコンピューティングセキュリティ要件ガイド

Version 1, Release 3 6 March, 2017

商標情報

この文書で参照された名称、製品、サービスは各々の所有者の商品名、商標またはサービスマークを含む場合がある。商用のベンダーや製品、サービスへの言及は、この文書の利用者への便宜だけを目的としたものであり、DoD、DISA、DISA リスク・マネジメント・エグゼクティブ (DISA RME) または連邦外の団体、イベント、製品、サービスまたは事業の DISA RME サイバー・スタンダード・ブランチによる承認を意味するものではない。

目次

第1章 はじめに.....	8
1.1 重要な用語	8
1.2 目的及び読者	9
1.3 権限	10
1.4 適用範囲	11
1.4.1 CC SRG と DoDI 8550.01 の適合性	14
1.5 セキュリティ要件ガイド (SRG) /セキュリティ技術実装ガイド (STIG)	14
1.6 SRG 及び STIG の配布	15
1.7 文書改訂と更新サイクル	16
1.7.1 コメント、改訂の提案および質問.....	16
1.8 文書構成	16
第2章 背景.....	17
2.1 クラウドコンピューティング、クラウドサービス及びクラウド開発モデル... 17	
2.2 クラウドサービスプロバイダ (CSP) とクラウドサービスの提供 (CSO)	20
2.3 DoD のリスクマネジメントフレームワーク (DoD RMF)	21
2.4 連邦のリスクと認可管理プログラム (FedRAMP)	21
2.5 FedRAMP Plus (FedRAMP+)	22
2.6 DoD 暫定認可.....	22
第3章 情報セキュリティの目的/影響レベル	23
3.1 セキュリティの目的 (機密性、完全性、可用性)	24
3.2 情報の影響レベル	26
3.2.1 レベル1：公開が許可された非格付け情報	27
3.2.2 レベル2：コントロール外の非格付け情報	27
3.2.3 レベル3：コントロールされた非格付け情報.....	27
3.2.4 レベル4：コントロールされた非格付け情報.....	27
3.2.5 レベル5：コントロールされた非格付け情報.....	30
3.2.6 レベル6：SECRET までの格付け情報.....	32
第4章 クラウドサービス提供のリスクアセスメント	32
4.1 商用/Non-DoD のクラウドサービスのアセスメント.....	33
4.2 DoD クラウドサービスとエンタープライズサービスアプリケーションのアセスメ ント	37
4.3 クラウドサービスの提供とミッションオーナーのリスク管理	39
4.3.1 クラウドコンピューティング、認可の境界.....	39
4.3.2 クラウドサービスの提供 (CSO) のリスク	41

4.3.3	ミッションリスク	41
4.4	CSM v2.1 から CC SRG v1r1 への CSP 移行およびその後の更新.....	43
4.4.1	CC SRG バージョン/リリースから更新された CC SRG バージョン/リリースへの CSP 移行	44
4.5	RFP への応募と契約獲得に関連した DoD PA ; DFARS の解釈.....	45
4.6	クラウドサービスとマネージド IT サービス	46
第5章	セキュリティに対する要求事項	48
5.1	セキュリティ管理策に対する DoD の方針.....	48
5.1.1	DoD における FedRAMP セキュリティ管理策の利用.....	48
5.1.2	DoD の FedRAMP+セキュリティ管理策/強化.....	49
5.1.3	セキュリティ管理策と強化のパラメータ値	52
5.1.4	国家セキュリティシステム (NSS)	53
5.1.4.1	NSS レベル 6 格付けオーバーレイの適用性.....	53
5.1.5	CNSSI 1253 プライバシー・オーバーレイ	53
5.1.5.1	レベル 2 における PII/PHI	54
5.1.5.2	CSP とミッションオーナーにおけるプライバシー・オーバーレイの影響.....	54
5.1.5.3	プライバシー・オーバーレイ管理策/強化の CS0 アセスメント	55
5.1.5.4	プライバシー・オーバーレイ管理策/強化のミッションシステム/アプリケーションアセスメント	56
5.1.6	契約/SLA のオプションで言及されるセキュリティ管理策/強化.....	56
5.1.7	L4/5 DoD PA 授与のための追加の考慮事項と要件	57
5.2	法的留意事項	60
5.2.1	管轄/所在地要件	60
5.2.1.1	DoD オフプレミス 対 オンプレミス 対 仮想オンプレミス	60
5.2.2	クラウド展開モデルの考慮事項/分離要件	63
5.2.2.1	影響レベル 2 場所と分離の要件	64
5.2.2.2	影響レベル 4 場所と分離の要件	64
5.2.2.3	影響レベル 5 場所と分離の要件	65
5.2.2.4	影響レベル 6 場所と分離の要件	66
5.2.2.5	法執行と刑事捜査と E ディスカバリの支援における分離	66
5.2.3	DoD データの所有権と CSP による DoD データの使用.....	67
5.3	継続的な評価	68
5.3.1	継続的モニタリング	69
5.3.1.1	DoD PA と FedRAMP カタログの CS0 の継続的監視.....	70
5.3.1.2	DoD で評価された CS0 の継続的なモニタリング.....	72
5.3.2	変更管理	73

5.3.2.1 DoD PA と FedRAMP カタログの CSO の変更管理	74
5.3.2.2 DoD で評価された CSO の変更管理	77
5.4 クラウドサービス提供者の DoD 公開鍵基盤(PKI)の利用	78
5.4.1 識別、認証、アクセス制御資格情報.....	80
5.4.1.1 CSP とミッションシステムインターフェースのミッションオーナー クレデ ンシャル	80
5.4.1.2 CSP 特権ユーザの資格情報	83
5.4.2 公開鍵 (PK) の有効化.....	84
5.5 方針、指針、運用上の制約事項.....	85
5.5.1 SRG/STIG コンプライアンス	85
5.6 物理的設備及び人的要件	86
5.6.1 施設要件	86
5.6.2 CSP 要員の要件.....	86
5.6.2.1 CSP 要員の要件 PS-2: 職位の分類	87
5.6.2.2 CSP 要員の要件 PS-3: 背景調査	89
5.6.2.3 CSP 要員に関するミッションオーナーの責任.....	92
5.6.2.4 トレーニング要件	92
5.7 データの流出	92
5.8 CSO から移行のためのデータ処理と破壊	95
5.9 記憶媒体及びハードウェアの再利用と破棄.....	96
5.10 アーキテクチャ	97
5.10.1 クラウドアクセスポイント(CAP:Cloud Access Point)	98
5.10.1.1 境界 CAP (BCAP)	100
5.10.1.2 内部 CAP (ICAP)	106
5.10.1.3 SIPRNet BCAP/ICAP	108
5.10.1.4 ミッションパートナーの環境またはコミュニティネットワークのクラウ ドアクセスポイント.....	109
5.10.1.5 クラウドでホストされている NIPRNet サービスへアクセスするミッシ ョンパートナーの環境.....	110
5.10.1.6 DISN BCAP を介したミッションシステムの接続承認.....	111
5.10.2 ネットワークプレーン.....	112
5.10.2.1 ネットワークプレーンの接続性.....	112
5.10.2.2 ユーザ/データプレーンの接続性.....	112
5.10.2.3 管理プレーンの接続性.....	115
5.10.3 CSP サービスアーキテクチャ	119
5.10.3.1 CSP サービスアーキテクチャ - SaaS	119

5.10.3.2 CSP サービスアーキテクチャ - IaaS/PaaS	121
5.10.3.3 CSP 被害復旧 (DR) - 運用の継続性 (COOP)	122
5.10.4 インターネットプロトコル (IP) のアドレス指定とドメインネームサービス (DNS)	122
5.10.4.1 IP アドレッシング	124
5.10.4.2 ドメインネームサービス (DNS)	127
5.10.5 SaaS を使用したミッションオーナーの要件 (全レベル)	129
5.10.6 IaaS/PaaS を利用したミッションオーナーのシステム/アプリケーションの要件	129
5.10.7 クラウドの Active Directory 統合	134
5.10.7.1 Active Directory フェデレーションサービス (ADFS)	135
5.10.7.2 Active Directory DirSync (ディレクトリ同期)	135
5.11 商用クラウドストレージにおけるデータの暗号化・保護	135
5.11.1 暗号消去	137
5.12 バックアップ	138
5.13 DoD 請負業者/DoD コンポーネントミッションパートナーによるクラウドサービスの利用	139
5.13.1 DoD コンポーネントミッションパートナー	139
5.13.2 Non-CSP DoD 請負業者および DIB パートナーによる CSP の利用による機密情報の保護	140
5.13.3 Non-CSO 製品またはサービスの一部として Non-CSP DoD 請負業者の CSP の利用	141
5.14 ミッションオーナーの DoD テストとクラウド上での開発	141
5.14.1 クラウドベースの T&D ゾーンへのワークステーションの接続性	144
5.15 ポート、プロトコル、サービス、管理およびクラウドベースのシステム/アプリケーション	146
5.16 モバイルコード	147
5.17 クラウドベースのシステム/アプリケーションの登録と接続承認	150
5.17.1 DISA システム/ネットワーク承認プロセス (SNAP)	150
5.17.2 DoD DMZ ホワイティスト	150
5.17.3 選択とネイティブプログラミングデータ入力システム - 情報技術 (SNaP-IT)	151
5.18 サプライチェーンのリスクマネジメントアセスメント	151
5.19 TASKORD 12-0920 に従った電子メールの保護	152
第 6 章 サイバー空間防衛とインシデントレスポンス	153
6.1 サイバー空間防衛の概要	154

6.2	クラウドコンピューティングにおける影響レベルのコンセプト変更	154
6.2.1	境界サイバー空間防衛アクション	155
6.2.2	ミッションサイバー空間防衛アクション	155
6.3	サイバー空間防衛アクション	156
6.4	サイバー空間防衛の役割と責任	157
6.5	サイバーインシデントの報告と対応	159
6.5.1	インシデントレスポンス計画と補遺	160
6.5.2	情報要件、カテゴリ、タイムライン、およびフォーマット	161
6.5.3	インシデント報告メカニズム	163
6.5.4	クラウドにおけるデジタルフォレンジックと法執行／犯罪捜査のサポート	164
6.5.4.1	悪意のあるソフトウェア	164
6.5.4.2	インシデント情報の収集、保存、および保護	164
6.5.4.3	LE/CI のためのフォレンジック／インシデント情報保管の継続性 (chain- of custody)	167
6.5.4.4	CSP による PA 取得に向けたデジタルフォレンジックサポート	167
6.6	警告、戦術的な指示と命令	168
6.7	継続的モニタリング／行動計画とマイルストーン (POA&Ms)	168
6.8	計画停止の通知	168
6.9	サイバー空間防衛のための PKI	169
6.10	脆弱性と脅威情報の共有	169
付録 A	参考文献	171
付録 B	用語集	176
付録 C	役割と責任	182
付録 D	PA の CSP 評価パラメータ値	186
付録 E	プライバシー・オーバーレイの C/CE 表と値の比較	313
付録 F	将来のプライバシー・オーバーレイガイダンス	344

表一覧

表 1	セキュリティ目標の潜在的な影響定義 (FIPS-199)	25
表 2	DoD FedRAMP+ セキュリティ管理策/強化	51
表 3	契約/SLA で対処されるセキュリティ管理策/機能強化	57
表 4	ミッションオーナー資格	81
表 5	ユーザ／データプレーンの接続性	112
表 6	管理プレーンの接続性	115

表 7 役割と責任	182
表 8 PA アセスメントのための FedRAMP M/FedRAMP+コントロール/強化: パラメータ値	187
表 9 表 3 に示された SLA コントロール/強化のパラメータ値	307
表 10 修正または規則から要求される FedRAMP M C/CE	313
表 11 FedRAMP+C/CE 修正または規制による要件	320
表 12 FedRAMP M または FedRAMP+に含まれない C/CE プライバシー・オーバーレイ	320
表 13 FedRAMP と FedRAMP+ C/CE の PII/PHI パラメータ値	325
表 14 FedRAMP M や FedRAMP+に含まれない C/CE の PII/PHI パラメータ値.....	338
図一覧	
図 1 影響レベルの比較	26
図 2 セキュリティ継承とリスクの概念的区分	42
図 3 継続的アセスメントの責任分担.....	68
図 4 FedRAMP JAB PA を有する CSO に対する DoD の継続的モニタリング	71
図 5 3PAO で評価された非 DoD 連邦機関 ATO による FedRAMP CSO の DoD 継続的モニタ リング	72
図 6 DoD がアセスメントした CSO に対する継続モニタリング.....	73
図 7 FedRAMP JAB PA を使用した CSP CSO の DoD 変更管理プロセス.....	75
図 8 3PAO 評価された連邦機関 ATO をもつ CSO に対する DoD 変更管理プロセス...	77
図 9 DoD 自己評価 CSP/CSO の DoD 変更管理プロセス	78
図 10 NIPRNet/商用/連邦クラウドエコシステム	98

第1章 はじめに

クラウドコンピューティングの技術とサービスは、国防総省 (Department of Defense) に、連邦政府全体の情報技術 (IT) 戦略と効率性イニシアチブに沿ったエンタープライズクラウド環境を展開する機会を提供している。クラウドコンピューティングは、部門がインフラストラクチャを統合し、コモディティの IT 機能を活用し、機能の重複を排除しながら業務の継続性を改善することを可能にする。これらのイニシアチブの全体的な成功は、DoD コンポーネントと業界で定義され理解されている、十分に実行されたセキュリティ要件に依存している。これらの要件の一貫した実装と運用は、ミッションの実行を保証し、機密データの保護を提供し、ミッションの有効性を高め、最終的に DoD が求めている成果と業務効率をもたらす。

商用クラウド・コンピューティング・サービスの取得と使用に関する最新ガイダンスに関する 2014 年 12 月 15 日の DoD CIO メモは、商用クラウドサービスを取得する際の DoD コンポーネントの責任を定義している。このメモでは、Federal Risk and Authorization Management Program (FedRAMP) およびこのクラウドコンピューティングセキュリティ要件ガイド (CC SRG) に記載されているセキュリティ要件に従って、コンポーネントが責任をもってクラウドサービスを最小限の経費で取得できるようにしている。以前、Defense Information Systems Agency (DISA) は、商用クラウドでクラウドセキュリティモデルを運用するための概念を発表した。バージョン 1 では全体的なフレームワークを定義し、公開データの初期ガイダンスを提供した。バージョン 2.1 では、管理された非格付情報 (Controlled Unclassified Information) の情報を追加した。CC SRG は、DoD のために DISA によって発行された他の SRG と同様の構成で、クラウドセキュリティ要件を文書化したものである。この SRG は、以前に公開されたクラウドセキュリティモデル (CSM) を基にして更新したものであり、CSM は廃版となる。

1.1 重要な用語

この CC SRG は、クラウドコンピューティングと DoD が利用している技術に関する特有の用語と概念を導入している。このセクションではいくつかの重要な用語を列挙しているが、コンテンツや要件の完全な理解を実現するために、このドキュメントを読む前に、またはこのドキュメントを読んでいる中で、定義については用語集である付録 B を参照されたい。

以下は、この文書全体で使用されている重要な用語のリストである。

- クラウドサービスプロバイダ (CSP)
- 商用 CSP
- DoD CSP
- Non-DoD の CSP

- クラウドサービスの提供 (CS0)
- DoD クラウドサービスカタログ¹
- DoD コンポーネント
- ミッションオーナー (MO)
- DoD プライベート CS0
- C/CE (コントロール/コントロール強化)
- DoD オフプレミス
- DoD オンプレミス
- DoD 仮想オンプレミス

1.2 目的及び読者

この CC SRG は、DoD がクラウドコンピューティングを活用するセキュリティモデルと、クラウドベースのソリューションを使用するために必要なセキュリティ制御および要件の概説である。

この CC SRG は、DoD が提供するクラウドサービスと、国防総省に代わって請負業者が提供するクラウドサービスに適用される。

CC SRG の役割は以下のとおりである：

- DoD クラウドサービスカタログへクラウドサービス提供者 (CS0) として掲載を希望する DoD および商用クラウドサービスプロバイダ (CSP) (DoD の契約業者) へセキュリティ要件とガイダンスの提供
- DoD が DoD または Non-DoD の CS0 のセキュリティ体制を評価し、CSP が DoD のミッションをホストできるように DoD 暫定認可 (PA) を与える決定を支援する根拠の確立
- DoD コンポーネントの認可当局 (AO) による DoD CSP の CS0 のセキュリティ体制の評価、DoD コンポーネントの CSP/CS0 による DoD コンポーネントの認可 (ATO) 決定の支援、および CS0 が他の DoD コンポーネントによって活用される場合の DoD の PA。 (たとえば、milCloud のための DISA の ATO/PA)
- DoD ミッションオーナーが DoD または商用クラウドサービスを使用および実装するための要件とアーキテクチャの定義
- DoD ミッションオーナー、SCA (セキュリティ管理策の評価者)、認可当局 (以前は承認と運用認可 (C&A) 職員)、および CS0 の使用を計画し承認するための指針の提供

¹ DoD Cloud Service Catalog:

(DoD CAC/PKI required) <https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Approved-Commercial.aspx>

(DoD CAC/PKI required) <http://www.disa.mil/~media/Files/DISA/Services/Cloud-Broker/AuthorizedCloudServicesCatalog.pdf> (Public)

- ・ DoD CIO（最高情報責任者）が DoD のウェブサイトおよびアプリケーションを、DoD 内のネットワークやデータセンターの物理サーバーから、DoD や商用 CSP が提供している仮想サーバーやネットワークで構成された低コストのコモディティ IT サービスを利用するクラウドイニシアチブへの移行のサポート
- ・ DoD CIO および連邦政府のデータセンター削減イニシアチブのサポート

この CC SRG の読者には以下を含む：

- ・ 民間および Non-DoD の CSP
- ・ CSP として運用する DoD プログラム
- ・ 商用/Non-DoD および DoD クラウド・コンピューティング・サービスを利用するか、またはその利用を検討している DoD コンポーネントおよびミッションオーナー
- ・ DoD のリスクマネジメントアセスメント当局と認定当局（A0）

1.3 権限

この文書は、DoD インストラクション 8500.01 および DoD インストラクション 8510.01 の権限の下で提供されている。

サイバーセキュリティと題する DoD インストラクション（DoDI）8500.01 は、DoD CIO の権限、指導及びコントロールの下で、コントロール相関識別子（CCI）、セキュリティ要件ガイド（SRG）、セキュリティ技術実装ガイド（STIG）、モバイルコードのリスクカテゴリ及び利用ガイドの開発維持を DISA ディレクターへ指示するものである。これは、DoD サイバーセキュリティの方針、標準、アーキテクチャ、セキュリティ管理策及び検証手順と一貫しており、国家安全保障局セントラルセキュリティサービス（NSA/CSS）の支援を受け、ステークホルダーからの意見も得ながら可能な限り自動化している。

DoDI 8500.01 は、責任を負う A0 によって文書化され承認された例外を除いて、該当する STIG、[NSA]セキュリティ構成ガイド、および SRG に従うことを確実にするために、DoD コンポーネントの方向性を指示するものがある。

DoD 8510.01 は、NIST Special Publication（SP）800-37、NIST SP 800-53、国家安全システム（CNSS）指令（CNSSI）1253、連邦情報セキュリティ管理法（FISMA）を実装し、DoD の IT に関する DoD リスクマネジメントフレームワーク（RMF）を確立し、関連するサイバーセキュリティの方針及び RMF を実行・維持するための責任を割り当てるものである。

1.4 適用範囲

DoDI 8510.01 の 2a 項において「この指示は、(2) DoD の情報を受信、処理、保存、表示、または送信するすべての DoD IT に適用される」と述べている。これらの技術は、DoD IS、プラットフォーム IT (PIT)、IT サービス、および IT 製品として大まかに分類されている。これには、研究、開発、テストおよび評価 (T&E) を支援する IT、DoD に代わって請負業者または他の団体が運営する DoD がコントロールする IT を含む。

DoDI 8510.01、Encl 3、3b 項 (13 ページ) は、内外の IT サービス (以前は「IT アウトソーシングプロセス」) を定義している。その性質上クラウドコンピューティングは、以下の定義に適合している。

3b. IT サービス。IT サービスはサービスユーザ組織の認可境界外にあり、サービスユーザの組織はアプリケーションや必要なセキュリティ管理策のアセスメントを直接制御することはできない。IT サービスを利用する DoD の組織は、通常、それを承認する (すなわち、承認決定を発行する) 責任はない。

(1) 内部 IT サービスは DoD IS によって提供される。内部 IT サービスを利用する DoD 組織は、サービスを提供する IS の種別が、サービスを利用する DoD IS のニーズに適合し、提供組織と受領組織の双方の役割と責任を記述した書面による合意を確実にしなければならない。

(2) DoD 以外の連邦政府機関が提供する外部 IT サービスを利用する DoD の組織は、情報を提供する IS の分類を情報とミッションの機密性、完全性、可用性のニーズに適合し、かつ IS が提供しているサービスは、その機関からの現在の許可の下で運用されていること。参考文献 (h) [ed. DoDI 8500.01]、省庁間の合意またはこれらの外部サービスに関する政府の作業範囲記述書には、適切なセキュリティ管理策の適用を含むサービスレベル契約 (SLA) の要件を含まなければならない。

(3) 商用その他の非連邦政府機関によって提供される外部 IT サービスを使用する DoD 組織は、サービスを提供する IS のセキュリティ保護が、DoD 組織の情報とミッションに関し、機密性、完全性、および可用性のニーズに適切であることを保証しなければならない。DoD 組織は、参考文献 (e) [ed. CNSSI 1253]に従って分類を実施し、提案の要求に含めるセキュリティ管理策のセットを適切に仕立てなければならない。DoD 組織は、サービスプロバイダ候補から提案されたセキュリティの妥当性を評価し、提案されたアプローチを受け入れるか、DoD の要求を満たすためにアプローチの変更

を交渉するか、または提案を拒絶する。承認されたセキュリティアプローチは、結果として生じる契約書または注文書で文書化されなければならない。

- (4) 商用クラウド・コンピューティング・サービスの形で外部 IT サービスを契約している DoD の組織は、DoD クラウドコンピューティングポリシーと手続きガイドラインを遵守している必要がある。

この CC SRG は、DoD 8510.01、Enc1 3、パラ 3b とともに、CSP の CS0 形式で内外の IT サービスにおける DoD ミッション・アプリケーションおよび DoD 情報をホストするための DoD セキュリティ目標を確立する。DoD 情報の秘密度は、公開可能なものから機密まで多岐にわたる。SECRET 以上のミッションは、既存の適用可能な DoD および情報機関（IC）の方針に従う必要があり、この CC SRG の対象外である。

注：IC は SECRET 以上の分類レベルで承認されたクラウドサービスを提供している。さらなる情報については、次の DoD CIO クラウドチームへ連絡：

osd.cloudcomputing@mail.mil.

この CC SRG は、所有者または運用者に関係なく、DoD システム/情報/データ/アプリケーションをホストしているすべての CSP/CS0 に適用される。所有者/運用者は、DoD のコンポーネント、連邦政府機関、または企業である。

この CC SRG は、44 USC 3534 (a) (1) (ii)（連邦情報セキュリティ管理法（FISMA））に基づいて DoD コンポーネントの長の責任をサポートし、「機関または機関の代理契約者やその他の組織によって利用・運用される情報システム」の防護を提供するものである。ミッションオーナーによって運用されていない CSP は、本質的に「機関の契約者」であり、「機関を代理して」情報システムを運用しているものである。CSP と契約しているミッションオーナーは、IT のワークロードの全部または一部を CSP に委託している。これは、DoDI 8510.01、Enc1 3、パラ 3b の「IT サービス」の利用と同じである。

この CC SRG は、クラウドサービスを使用するすべての DoD ミッションオーナー、および DoD ミッションオーナーにクラウドサービスのプロビジョニングに関与するすべての関係者にも適用される。これにはインテグレータまたはブローカおよび主契約者として機能する CSP や、同様にサポートしている CSP または設備のプロバイダ（例えば、下請け業者）を含み、インテグレータ／ブローカ／CSP は DoD の契約のもとで完全なサービスまたは一連のサービスを提供するために活用もしくは契約している。例えば、CSP A が CSP C のデータセンターに所在した CSP B が提供する IssA の中で SaaS のインスタンスを生成した場合、CC

SRG はこれら 3 件の CSP/CSO に適用要件として適用可能である。同様に、完全な契約要件に対し利用、再販または複数の CSP/CSO によるクラウド・サービス・インテグレーター/ブローカについても CC SRG はすべてのクラウドサービスに適用できる。CSP の全体的なサービス提供は第三者からのコントロールとコンプライアンスを継承しているかもしれないが、サービスのために DoD との契約を有する CSP は、最終的にコンプライアンスの完全な責任を負う。この適用性に関する声明および関連する要件は、DoD 請負業者（この場合はインテグレーター/ブローカ/CSP）がすべての下請け契約において現存するすべてのセキュリティ要件を含まなければならないと規定している DoD および連邦取得要件および条項と一致している。

商用および Non-DoD の CSP の認可プロセスは、FedRAMP の使用による FISMA および NIST RMF プロセスに基づいており、セクション 4「本書のクラウドサービス提供のリスクアセスメント」で概説されている DoD の考慮事項が補足されている。これらの要件と考慮事項は、DoDRMF の要件の一部である。クラウド機能またはサービス提供（例：milCloud、Defense Enterprise Email）を提供する DoD エンタープライズサービスプログラムのプロセスは、FISMA および NIST RMF プロセスと同様の DoD RMF 要件およびプロセスに基づいている。どちらのプロセスも、NIST SP800-53 のセキュリティ管理策のベースラインをアセスメントの基礎として利用し、DoD がリスクのレベルを決定できる共通の枠組みを提供している。この SRG は、Non-DoD のソフトウェアをサービス（SaaS）として契約し使用する場合、DoD または Non-DoD のインフラストラクチャとしてサービス（IaaS）およびプラットフォームとしてサービスを提供（PaaS）する場合に、DoD ミッションオーナーに対する DoD ベースラインセキュリティ要件を確立する。IaaS と PaaS は CSP の顧客がこれらのサービスの上にシステムまたはアプリケーションを構築することから、この CC SRG のリリースでは、IaaS と PaaS は似ているとみなされ、特に断りのない限り同じ方法で扱っている。SaaS は、他のアプリケーション関連の SRG と STIG で特定のアプリケーション要件が特定されている他のサービスモデルの範囲に対応している。

注：PaaS CSO には、ミッションオーナーにはセキュリティ対策の無いプログラミング環境と OS だけが提供されて自らがセキュリティ保護を行う必要があるものから、SaaS に非常に近く CSO がほぼアプリケーションを完成させているため、ミッションオーナーはそのインターフェースのカスタマイズだけが許されるものまで幅があることを踏まえ、PaaS については、今後の CC SRG でよりの確に言及される。

注：この CC SRG は、クラウドコンピューティングのすべての DoD の利用形態に適用されるが、この SRG の主要な焦点の 1 つは、DoD コンポーネントが所有し、DoD 防衛情報システムネットワーク (DISN) サービス（例えば Non セキュアー・インターネットプロトコルルータネットワーク (NIPRNet)）及びセキュアー・インターネットプロトコルルータネットワーク

(SIPERNet)) と DoD または Non-DoD のクラウドサービス (NIST で定義されている) へ接続した、物理インフラストラクチャ (仮想か否かによらず) でホストされている DoD システムとアプリケーションの移行を容易にすることである。この定義については、セクション 2.1、クラウドコンピューティング、クラウドサービス、クラウド展開モデルを参照。この SRG は、DoD や Non-DoD のクラウドサービスに移行しているか利用していない限り、また DoD または DoD 以外のシステムや DoD で使用されているインターネット上の直接アクセスが承認されているアプリケーションに対処しない限り、インターネットを介して直接アクセスできる商用クラウドサービスに移行していない限り (DISN を通過しない)、全ての DoD システムおよびアプリケーションに対応するものではない。この SRG は、そのようなクラウドサービスとそれを使用するアプリケーションを評価/承認するために使用されることがあるが、使用する承認済みのネットワークアクセスまたは接続方法を変更することを意図するものではない。

1.4.1 CC SRG と DoDI 8550.01 の適合性

DoDI 8550.01 「DoD インターネットサービスとインターネットベースの機能」(2012 年 9 月 11 日)²は、「インターネットベースの機能 (IbC) を使用して、非格付け DoD 情報の収集、配布、保存、処理」に言及している。このポリシーの目的は、DoD コンポーネントとユーザがインターネット上で確立しているさまざまな公的サービスの利用を可能にすることである。主な利用事例の 1 つは、広報コミュニケーションキャンペーンの一環として、これらのサービス (Facebook や Twitter など) による公開情報の配布である。次の利用形態として、ブログの発行が含まれる。DoDI 8550.01 がカバーするすべての情報の DoD 情報影響レベルは、レベル 2 である。

DoDI 8550.01 が扱うサービスはクラウドサービスと見なすことができるが、典型的な資金調達モデルは、そのようなサービスを無料で利用でき、そのモデルに基づいて広く一般に使用されている。さらに、これらのサービスは DoD や、または DoD のプロバイダによって管理されていないため、DoD の RMF 要件は適用されない。逆に、CC SRG は、DoD ポリシーで DoD ATO を必要とするすべてのクラウドサービスに適用される。これには、DoD システムが構築 (DoD による、または DoD のために) される、すべての IaaS および PaaS の CSO を含む。

1.5 セキュリティ要件ガイド (SRG) /セキュリティ技術実装ガイド (STIG)

セキュリティ要件ガイド (SRG) は、テクノロジーファミリー、製品カテゴリ、または組織全般に適用されるセキュリティ要件の集合体である。SRG は、IT システムおよびアプリケーション

² DoDI 8550.01: <http://www.dtic.mil/whs/directives/corres/pdf/855001p.pdf>

ョン全体で共通して発生するセキュリティ上の脆弱性の原因を軽減するために、製品に依存しない要件を提供している。

SRG が様々な技術ファミリーや組織に対する高レベルの要求を定義しているが、STIG は製品特有の詳細なガイドラインとなっている。言い換えれば、STIG は、SRG で定義されている要件をその製品の技術分野に準拠させ、検証し、達成し、継続的に維持するための製品固有の情報を提供している。

一つの技術に関連した SRG または STIG は、特定のシステムにおいて、すべてを含むわけではない。システムに適用可能なすべての SRG/STIG への準拠が必要である。すなわち、典型例としては、あるシステムが結果として複数の SRG や STIG の対象となる。

新しく発行された SRG と STIG は、一般に、テクノロジー/製品概要ドキュメントと、セキュリティ要件を含むエクステンシブル・コンフィグレーション・チェックリスト記述形式 (XCCDF) の 1 つ以上のエクステンシブル・マークアップ言語 (XML) ファイル (.xml) で構成される。セキュリティ要件は、Control Correlation Identifier (CCI) の形式で提示され、製品固有の構成と検証手順が含まれる。この CC SRG の要件は、現時点では XCCDF XML 形式で公開されていない。

SRG と STIG に含まれるセキュリティ要件は、一般に、すべての DoD 管理システム、DoD ネットワークに接続されているすべてのシステム、および DoD のために運用・管理されているすべてのシステムに適用される。この要件は、クラウドサービスのシステムを構築しているすべてのミッションオーナーに有効である。CSP のシステムは、STIG/SRG を利用することにより、NIST SP 800-53 コントロール CM-6 と整合した構成ガイダンス、または DoD から同等とみなされる構成ガイドに準拠しなければならない。

1.6 SRG 及び STIG の配布

関係者は、情報保証サポート環境 (IASE:Information Assurance Support Environment) のウェブサイトから該当する SRG と STIG を入手することができる。秘区分なしのウェブサイトは <http://iase.disa.mil>、秘区分のあるウェブサイトは <http://iase.disa.smil.mil> である。

注：一部のコンテンツをアクセスするには、DoD 公開鍵インフラストラクチャ (PKI) 証明書が必要である。IASE ウェブサイトは現在、外部認証局 (ECA:External Certificate Authority) の証明書を PKI 保護領域に登録することはできない。PKI 制限付きコンテンツを必要とする業界のパートナーは、DoD スポンサーを通じて要求することができる。

1.7 文書改訂と更新サイクル

DISA リスク・マネジメント・エグゼクティブ・サイバーセキュリティ・スタンダード支部は、必要に応じて SRG および STIG の文書を四半期毎のメンテナンス・リリース・スケジュールで作成、改訂、更新、公開している。これらの出版物は、新しくまたは変更されたポリシー、要件、脅威、または緩和策、再編成されたコンテンツ、誤りの訂正を反映し、またはさらなる明瞭性を提供している。会計年度ベースの発行スケジュールは <http://iase.disa.mil/stigs/Pages/fso-schedule.aspx> で閲覧可能である。

SRG または STIG の改訂版が発行されると、追録リリースではなくバージョンの変更となる。新しい SRG と STIG 及び主要な更新は、承認されて公開準備が整い次第、直ちにリリースされる。

1.7.1 コメント、改訂の提案および質問

コメント、改訂の提案および質問は、電子メール(disa.stig_spt@mail.mil)でいつでも受理される。

DISA リスク・マネジメント・エグゼクティブ・サイバーセキュリティ・スタンダード支部は、メンテナンス・リリースまたはメジャー・アップデートへの包含、発行に先立って、関連する DoD 組織とすべての変更要求を調整する。

1.8 文書構成

この SRG は、6 つの主要セクションと付録で構成されている。セクション 1～4 は、特定の CSP のクラウド提供を認可するプロセスを含む一般的な情報に関するものである。残りのセクションでは、クラウド機能の認可と運用において取り組むべき特定のセキュリティ要件について概説している。SRG の役割と責任、および必要なコントロールパラメータ値の詳細に加えて、付録では、文書全体で使用される引用情報と用語の定義を提供している。

第 1 章、はじめに：このドキュメントの目的と利用に関する一般的な情報を提供している。

第 2 章、背景：文書全体で使用されているいくつかの用語と関連する概念に関する入門編である。

第 3 章、「情報セキュリティ目標/影響レベル」：クラウドでホストされているデータのタイプに基づいて「情報影響レベル」の概念を説明し、機密性、完全性、および可用性の分野におけるセキュリティ対策方針の概要を説明している。

第4章、クラウドサービス提供のリスクアセスメント：DoD PAを得るために使用されるRMFプロセスの概要と、ATO決定を支援するためにミッションオーナーとそのAOがPAをどのように活用できるかを説明している。

第5章、セキュリティ要件：CSP機能を有効にするための要件を詳述している。

第6章、サイバー空間防御とインシデントレスポンス：DoD ミッションシステムを守り運用するために必要なコマンド&コントロール (C2) のプロセスとともに、クラウドで動作する情報システムの防御に関する要件の概要を説明している。

第2章 背景

本章ではこの文書の入門編として、様々な概念、用語及び関連したプロセスを概説する。

2.1 クラウドコンピューティング、クラウドサービス及びクラウド開発モデル

NIST SP800-145³では、クラウドコンピューティングが持つ5種類の主要な特徴、3種類のサービスモデル及び4種類の展開モデルを定義している。このSRGは、クラウドコンピューティングの議論を特徴づけて標準化するために、これらのNIST定義に準拠している。クラウドコンピューティングは次のように定義されている。

クラウドコンピューティングは、マネジメント作業やサービスプロバイダとのやりとりを最小限に抑えて迅速にプロビジョニングしてリリースできる構成可能なコンピューティングリソース（ネットワーク、サーバー、ストレージ、アプリケーション、サービスなど）の共有プールに、ユビキタスで便利なオンデマンド・ネットワーク・アクセスを可能にするモデルである。

基本的な特徴は次のとおり。

オンデマンドセルフサービス：利用者は、各サービスプロバイダの人とやりとりせずに、必要に応じてサーバーの利用時間やネットワークストレージなどのコンピューティング能力を自動的に利用することができる。

³ NIST SP 800-145: <http://csrc.nist.gov/publications/PubsSPs.html>

広範なネットワークアクセス：ネットワークを介して、シンクライアントプラットフォームを含む様々な機種（例えば、携帯電話、タブレット、ラップトップ、ワークステーションなど）の使用を促進する標準的なメカニズムを通じてアクセスできる。

リソースプール：プロバイダのコンピューティングリソースは、マルチテナント・モデルを使用して複数の利用者へサービスを提供するためにプールされ、異なる物理・仮想リソースが利用者の要求に応じて動的に割り当てられ、再割り当てされる。地理的な場所に依存しない特徴があり、利用者は、一般に、提供されるリソースの正確な場所を指定することや、その場所を知ることができないが、より高い抽象レベル（例えば、国、州またはデータセンター）で場所を指定することは可能である。リソースの例には、ストレージ、処理、メモリ、ネットワーク帯域幅などがある。

迅速な柔軟性：能力は柔軟に供給され、場合によっては自動的に解放され、需要に見合うように迅速に拡張または縮小することができる。利用者からは、利用できる能力が無制限であるように見え、いつでも必要なだけ充当できる。

計測されたサービス：クラウドシステムは、サービスのタイプ（ストレージ、処理、帯域幅、アクティブなユーザ数など）に適した抽象レベルの測定機能を活用することによって、リソースの使用を自動的に制御・最適化を行う。リソースの使用状況を監視、制御、報告することができ、利用しているサービスの提供者と利用者の両方に透明性を確保している。

NIST で定義されているクラウドサービスモデルには、SaaS (Software as a Service)、PaaS (Platform as a Service)、IaaS (Infrastructure as a Service) があり、以下のよう

サービスとしてのソフトウェア (SaaS)：利用者に提供される機能は、クラウドインフラストラクチャ上で実行されているプロバイダのアプリケーションの使用である。アプリケーションは、ウェブブラウザ（例えば、ウェブベースの電子メール）のようなシンクライアントインタフェースまたはプログラムインタフェースを介して、様々なクライアント機器からアクセス可能である。ユーザは、ネットワーク、サーバー、オペレーティングシステム、ストレージ、さらには個々のアプリケーション機能を含む基盤となるクラウドインフラストラクチャを管理したり制御したりすることはない。

サービスとしてのプラットフォーム (PaaS)：利用者に提供される機能は、プロバイダがサポートするプログラミング言語、ライブラリ、サービス、およびツールを使用して利用者

が作成または取得したアプリケーションを、クラウドインフラストラクチャに展開することである。利用者は、ネットワーク、サーバー、オペレーティングシステム、ストレージなどの基盤となるクラウドインフラストラクチャを管理または制御することはないが、展開されたアプリケーションやアプリケーションホスト環境の構成を設定するための制御は可能である。

サービスとしてのインフラストラクチャ (IaaS) : 利用者に提供される機能は、利用者がオペレーティングシステムおよびアプリケーションを含む任意のソフトウェアを展開して実行可能な、処理、ストレージ、ネットワーク、および他の基本的なコンピューティングリソースを提供することである。利用者は、基盤となるクラウドインフラストラクチャを管理または制御するのではなく、オペレーティングシステム、ストレージ、および展開されたアプリケーションの制御を行う。ただし、ネットワークの構成要素（例えば、ホストファイアウォール）の制御が制限される可能性がある。

NIST は、以下のようにクラウド展開モデルを定義している。

プライベートクラウド : クラウドインフラストラクチャは、複数の利用者（例えば、ビジネスユニット）を含む単一の組織によって排他的に使用されるようにプロビジョニングされる。プライベートクラウドは、組織、第三者、またはそれらの組み合わせによって所有、管理、運営され、オンプレミスまたはオフプレミスで設置される。

コミュニティクラウド : クラウドインフラストラクチャは、関心事項（例えば、ミッション、セキュリティ要件、ポリシー、コンプライアンスの考慮事項）を共有している組織の特定の利用者コミュニティによって独占的に使用されるようにプロビジョニングされている。コミュニティ、第三者、またはそれらの組み合わせの 1 つまたは複数の組織によって所有、管理、および運用されていても構わないし、オンプレミスまたはオフプレミスの場合もある。

パブリッククラウド : クラウドインフラストラクチャは、一般の人々がオープンに使用できるように準備されている。パブリッククラウドは、ビジネス、アカデミック、または政府組織、またはそれらのいくつかの組み合わせによって所有、管理、および運営されることがあり、クラウドプロバイダのオンプレミスとして所在している。

ハイブリッドクラウド : クラウドインフラストラクチャは、固有のエンティティのままであるが、データとアプリケーションの移植性を可能にする標準化されたまたは独自のテクノロジーによって結合された 2 つ以上の異なるクラウドインフラストラクチャ

(プライベート、コミュニティ、またはパブリック)の構成である(たとえば、クラウド間の負荷分散のためのクラウド拡張)。

この SRG では、プライベートとコミュニティについて次の意味としている。「DoD プライベート/コミュニティクラウド」は、DoD ユーザまたはテナント専用構築されたクラウドサービスを示す。「連邦政府コミュニティクラウド」は、DoD と他の連邦政府のテナントを含むものである。たとえば、陸軍と空軍のテナントのみが使用するクラウドは DoD のプライベート/コミュニティとみなされ、DISA と国務省が利用するクラウドは連邦政府のコミュニティクラウドとなる。

ベンダーは、提供するサービスに好きな名称を付けてマーケティングしているかもしれないが、DISA は、DoD クラウドサービスカタログに掲載する際に、3 つの NIST クラウドサービスモデルの中の 1 つに分類している。ベンダーは、NIST クラウドサービスモデルの用語を使用してサービスを販売することが推奨される。コンピューティングサービスを提供せずにデータストレージを提供するサービス提供は、IaaS のサブセットであるとみなされる。さらに、ベンダーによって提案された他のサービスモデル(Data as a Service (DaaS) など)は、3 つの標準的なサービス提供モデルの 1 つに合わせて、適切なコントロールを満たす必要がある。この SRG で使用されているように、クラウドコンピューティングおよびクラウドサービスという用語は、プロバイダ組織から 1 つ以上の組織の顧客またはテナント組織に提供されるサービスを示す。これらの用語は、専用のハードウェア(仮想化されているかどうかにかかわらず)が組織によって使用または組立てられて使用される従来の形式の IT サービス配信を示さない。プロバイダ組織から顧客に提供されるサービスは、この構成概念の一部でなければならない。

2.2 クラウドサービスプロバイダ (CSP) とクラウドサービスの提供 (CSO)

クラウドサービスプロバイダ (CSP) は、1 つ以上の展開モデルで 1 つ以上のクラウドサービスの提供者である。CSP は、他の組織や他の CSP のサービス(例えば、データセンター、通信事業者のホテル/コロケーション施設、IXP などの第三者施設に特定のサーバーまたは機器を設置するなど)を活用またはアウトソーシングする可能性がある。SaaS を提供する CSP は、1 つ以上の第三者 CSO (すなわち、IaaS または PaaS) を活用して、機能の構築または提供を行う可能性がある。

クラウドサービスの提供 (CSO) は、CSP から入手可能な実際の IaaS/PaaS/SaaS ソリューションである。CSP はいくつかの異なる CSO を提供する可能性があるため、この区別は重要である。

2.3 DoD のリスクマネジメントフレームワーク (DoD RMF)

DoDI 8510.01 は、DoD RMF(Risk Management Framework)の方針を実装し、関連するサイバーセキュリティポリシーの確立、RMF の実行と保守の責任の割り当てを行っている。この DoD の方針は、NIST SP 800-37「連邦政府の RMF を定義するリスク管理フレームワークの適用ガイド」と一貫性を持っている。CNSSI 1253 および NIST SP 800-53、連邦情報システムおよび組織のセキュリティおよびプライバシーコントロールは、この DoD ポリシーに組み込まれており、アセスメントプロセスで使用するコントロールおよびコントロールベースラインの概要を示している。この SRG にとって非常に重要なことは、DoDI 8510.01 が、情報システム (IS) の認可と接続のために、DoD と他の連邦機関との間の承認決定と成果物を相互に受け入れるための DoD 内の手続きのガイダンスを提供していることにある。

2.4 連邦のリスクと認可管理プログラム (FedRAMP)

Federal Risk and Authorization Management Program⁴ (FedRAMP) は、連邦政府が使用するクラウド製品とサービスのセキュリティアセスメント、認可、継続的な監視に対する標準化されたアプローチを提供する政府全体のプログラムである。FedRAMP は、連邦政府の Cloud-First イニシアチブのもとで、システムとアプリケーションが商用クラウドに移行されるよう、行政管理予算局 (OMB: Office of Management and Budget) によってすべての連邦政府機関に対して使用を義務付けられている。2011 年 12 月の OMB FedRAMP 方針メモ⁵では、連邦部門と機関に対し、FedRAMP で認定された CSP を利用し、機関の ATO を FedRAMP セキュア・リポジトリと共有することを要求している。

FedRAMP は、セキュリティアセスメントやプロセスモニタリングレポートに必要なコスト、時間、要員の削減を目的として「一度作って、何回も使用する」フレームワークを使用している。FedRAMP Joint Authorization Board (JAB) は、FedRAMP プログラムの主要なガバナンスおよび意思決定機関である。JAB が承認した基準とプロセスは、連邦政府のミッションをホストする PA の獲得と維持をもたらす。

DoD は、DoD の PA について CSO のアセスメントを行う際のすべてのサポート文書を含み、FedRAMP JAB PA および Non-DoD の連邦機関 ATO パッケージ (FedRAMP セキュア・リポジトリにある) を活用している。しかし、DoD は、CSP/CSO が FedRAMP 認定の第三者機関 (3PAO) によって評価された Non-DoD の機関の ATO のみを受理している。

⁴ FedRAMP: <https://www.fedramp.gov/>

⁵ December 2011 OMB Policy Memo: <https://www.fedramp.gov/files/2015/03/fedrampmemo.pdf>

注：American Association for Laboratory Accreditation⁶ (A2LA) は、FedRAMP プログラム管理室 (PMO) の承認を得て FedRAMP 3PAO の認定を行う。

2.5 FedRAMP Plus (FedRAMP+)

FedRAMP+は、FedRAMP アセスメントの一環として行われた作業を活用し、DoD の重要任務要件を満たすために必要な特定のセキュリティ管理策と要件を追加するコンセプトである。CSP の CSO は、本 SRG で概説された基準に従って評価され、その結果は DoD 暫定認可授与の基礎として使用される。

2.6 DoD 暫定認可

DoD 暫定認可 (PA) は、CSP の CSO によるリスクベースの評価と DoD ネットワークにもたらされるリスクの可能性についての認定である。DoD PA プロセスは FedRAMP と同様に「一度作って、何回も使用する」フレームワークに従っている。DoD PA はすべての情報影響レベルについて付与される。PA はミッション・アプリケーションを担当する A0 が、CSO の一部として実行されるミッション・アプリケーションの全体的なリスクを決定する際に活用しなければならない基盤を提供している。

CSP によって提供される CSO のすべてがアセスメントのために提出されていない可能性があるため、DoD PA は CSP 自体ではなく CSO に対する CSP へ付与される。さらに、CSP の CSO が別の CSP の CSO を活用する場合（例えば、CSP A が CSP B の IaaS 製品で SaaS 製品をインスタンス化）、CSP A の CSO に対する DoD PA は CSP B の継承されたコンプライアンスを含む。この場合、CSP A は CSP B についても契約上の責任を負い、その下請け契約に対するコントロールについて説明責任を持たなければならない。したがって、DoD にサービスを提供する CSP は、DoD PA を持っている他の CSO だけを利用することを強く推奨する。活用する CSP/CSO に PA がない場合、それはプライム CSO の一部として評価される。このように部分評価されたアセスメントは、活用する CSP/CSO に独立した PA を自動的に付与するものではない。DoD PA の評価の際に、CSP は DoD に提供された CSO で使用される下請け CSO を開示しなければならない。

注：施設が複数の CSP または複数のテナントの機器をサポートしている場合、CSO とみなされても、DoD PA はクラウドインフラストラクチャをサポートする物理的な施設（データセンターなど）には付与されない。これらは、秘密区分のない施設に対する 3PAO の CSP の CSO の一部としての物理的および環境的コントロールのために評価される。秘密区分のある処理施設は、この CC SRG の後半で扱われる。

⁶ American Association for Laboratory Accreditation: <https://www.a2la.org/>

DoD PA は、CSP/CSO が FedRAMP PA を失った場合、または CSP がこの CC SRG で特定されたセキュリティ責任、他の参照文書に記載されている関連要件、または契約要件を遵守しない場合に取り消すことができる。さらに、DoD PA を持つ他の CSP の CSO を活用している DoD PA を持つ CSP の CSO は、活用している CSO が PA を失うと PA を失う可能性がある。プライム契約者としての CSP は、CSO の PA を維持し、すべての下請け CSP に、契約期間中の CSO の PA を維持するよう要求しなければならない。このフロー・ダウンは、プライム・コントラクターとして機能するクラウド・サービス・インテグレーターおよびブローカにも適用できる。プライムまたは下請け契約 CSO が PA を失い、その是正を拒否、または是正できない場合、そのような状態は契約違反となる可能性がある。PA を取り消すことは極端な対策であり、DoD は CSP と協力して取り消しにつながる問題の是正に努める。2014 年 12 月の DoD CIO メモに従って⁷、DISA AO は DoD PA の承認と取り消しを担当している。

DoD PA を保有する CSO は、DoD クラウドサービスカタログ⁸にリストされている。DoD コンポーネントサービスは、当該機関の使用のために承認済みの CSP/CSO リストを実装することができる。

第3章 情報セキュリティの目的/影響レベル

クラウドセキュリティ情報の影響レベルは、次の組み合わせによって定義されている。1) CSP 環境で保存および処理される情報（例えば、公的、私的、秘密区分など）の機微性または機密性レベル；2) その情報の機密性、完全性、または可用性の喪失がもたらす事態の潜在的影響度。DoD ミッションの所有者は、DoDI 8510.01 および CNSSI 1253 に従ってミッション情報システムを分類し、定義された分類と情報の機密性に最も近いクラウド情報影響レベルを特定する必要がある。クラウド情報影響レベルは、3.2「情報影響レベル」でさらに定義されている。

⁷ Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services: http://dodcio.defense.gov/Portals/0/Documents/Cloud/DoD%20CIO%20-%20Updated%20Guidance%20-%20Acquisition%20and%20Use%20of%20Commercial%20Cloud%20Services_20141215.pdf

⁸ DoD Cloud Service Catalog: <https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Approved-Commercial.aspx> (DoD CAC/PKI required)
<http://www.disa.mil/~media/Files/DISA/Services/Cloud-Broker/AuthorizedCloudServicesCatalog.pdf> (Public)

3.1 セキュリティの目的（機密性、完全性、可用性）

情報影響レベルは、機密性または情報の完全性が損なわれた場合の潜在的な影響を考慮している。

連邦情報処理標準（FIPS）刊行物 199、連邦情報と情報システムのセキュリティ分類の基準⁹によると、機密性は、「個人のプライバシーや知財情報を保護するための手段を含む、情報のアクセスと開示に関する許可された制限を保持する...」[44 U.S.C., Sec. 3542]¹⁰とされている。機密性の喪失は、許可されない情報の開示である。

FIPS 刊行物 199 は、完全性を「不適切な情報の変更または破壊から保護し、情報の否認防止と信頼性を保証することを含む」と定義している[44 U.S.C., Sec. 3542]。完全性の喪失は、許可されていない情報の変更または破壊である。許可されていない情報の破壊が、その情報の可用性を失うことになることにも注意することが重要である。

FIPS-199 では、機密性や完全性の喪失の影響を示すために 3 つのレベルを定義している（表 1 参照）。すべての影響レベルのセキュリティ管理策基準は、中程度の機密性と中程度の完全性に基づいている。ミッションオーナーが潜在的に高い影響を持つ場合、DoD RMF を通じて CNSSI 1253 の高いベースラインを使用して評価された DoD 施設に展開するか、このリスクを対処/緩和するために、契約/SLA に特定の要件を含める必要がある。将来、DISA は FedRAMP 高ベースラインをこの SRG に組み込むことを検討している。

⁹ FIPS 199: <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

¹⁰ 44 U.S.C., Sec. 3542: <http://www.gpo.gov/fdsys/granule/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542>

表 1 セキュリティ目標の潜在的な影響定義 (FIPS-199)

セキュリティ の目的	影響の度合い		
	低	中	高
機密性	許可されていない情報の開示は、組織の業務、組織の資産、または個人に限定的な悪影響を及ぼすことが予想される。	許可されていない情報の開示は、組織の業務、組織の資産、または個人に重大な悪影響を及ぼすことが予想される。	許可されていない情報の開示は、組織の業務、組織の資産、または個人に重大または致命的な悪影響を及ぼすことが予想される。
完全性	情報の不正改ざんや破壊は、組織の業務、組織の資産、または個人に限定的な悪影響を及ぼすことが予想される。	情報の不正改ざんや破壊は、組織の業務、組織の資産、または個人に重大な悪影響を及ぼすことが予想される。	情報の不正改ざんや破壊は、組織の業務、組織の資産、または個人に重大または致命的な悪影響を及ぼすことが予想される。

FedRAMP のベースラインでは可用性に言及している中で、DoD クラウドのベースラインでは、可用性の影響を追加的には扱わない。ミッションオーナーが CSP を選ぶ際に CS0 が定める可用性の程度を評価することを期待している。特定のまたは追加の可用性要件は、契約または CS0 とのサービスレベル契約に含める必要がある。ミッションオーナーは、必要な可用性を確保するために、文言が特定かつ包括的であることを保証する必要がある。たとえば、「システムの可用性に影響を及ぼす CSP による保守は 4 週間前に調整されなければならない、1 か月に 4 時間を超えない」という要件の場合、契約/SLA で要件を詳述する必要がある。推奨される契約/SLA の可用性コントロールは、5.1.6 項、契約/SLA の中でオプションなるセキュリティ管理策／強化の下で提供される。

可用性は CS0 がアセスメントプロセスの一部として評価を行う。アセスメントされた可用性のレベルは、DoD クラウドサービスカタログにリストされる。この評価は、CS0 が PA を取得すること、または DoD クラウドサービスカタログに含まれることを妨げるものではない。DoD ミッションオーナーの要求を満たす 1 つ以上の適切なクラウドサービスとのマッチングを容易にするためにのみ使用される。

3.2 情報の影響レベル

以前に公表されたクラウドセキュリティモデル¹¹（現在は置き換えられた）では、6つの情報影響レベルが定義されている。選択プロセスを簡素化するために、レベル数は6から4に減少させた。レベル1（公開情報）とレベル3（低インパクトCUI）をそれぞれレベル2とレベル4に統合することによって達成された。影響レベル2、4、5、および6を残し、以前のバージョンのクラウドセキュリティレベルとの一貫性を維持するために、影響レベルの数値指定子に変更されていない。高いレベルでは、低いレベルからのデータの処理が可能である。

さらに、すべてのレベルのクラウドに格納、処理、または送信される情報の分類は、CNSSI 1253 で定義されている中程度の機密性と中程度の完全性に変更されている。この高機密性と高完全性からの影響レベル5および6への変更は、商用CSP施設に展開されるほとんどのDoD顧客システムの分類とより一致するように意図されている。

高機密性や高完全性の影響レベルに分類されたシステムおよび情報を持つミッションオーナーは、CNSSI 1253 高ベースラインで評価されたDoD RMF（通常はDoD施設）に展開するか、または商用CSPからセキュリティを追加して契約しなければならない。DISAは、このSRGへFedRAMP高ベースラインを組み込む方法を検討している。

図1は、現在のインフォメーション・影響レベルの要約と、いくつかの識別要件および特徴を示している。

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

図1 影響レベルの比較

注:5.2.1, "US/US 外地域" についての所轄/所在地要件を参照

¹¹ Cloud Security Model: http://iase.disa.mil/cloud_security/Pages/archive.aspx

注:ADP-1 と ADP-2 の要員に対する要求は影響レベル 4 と 5 の両方に適用である。

5.6.2, .1,.2,.3 参照

注:レベル 4/5 オフプレミス CSO の接続性は、それがサービスする任意の DISN ネットワーク（例えば DREN）上の BCAP を経由して行われる。

以下のサブセクションは、以前に使用された影響レベルと、ミッションオーナーが CSO に保管またはホストする情報のタイプを含めた影響レベルの説明である。

3.2.1 レベル 1：公開が許可された非格付け情報

レベル 1 は使用されなくなり、レベル 2 と統合された。

3.2.2 レベル 2：コントロール外の非格付け情報

レベル 2 には、公開が許可されたすべてのデータが含まれると同時に、コントロールされた非格付け情報（CUI）、または重要な軍事/非常事態の運用ミッション・データとして指定されていないが、最小限のレベルのアクセス制御（例えばユーザ ID とパスワード）を必要とされるデータを含む。このレベルは、CNSSI-1253 に基づき、低い機密性で中程度の完全性（L-M-x）に基づく非格付け情報の分類に対応している。

商用レベル 2 の CSP/CSO の顧客には、政府の顧客、商用の顧客および一般市民を含み、CSP が、CSO を販売することを選択した人が含まれる。CSO へのアクセスはインターネット経由で行われる。

3.2.3 レベル 3：コントロールされた非格付け情報

レベル 3 は使用されなくなり、レベル 4 と統合された。

3.2.4 レベル 4：コントロールされた非格付け情報

レベル 4 は、CUI やその他のミッションクリティカルなデータに対応し、軍事または非常事態の運用を直接支援するものを含んでいる。CUI は、連邦政府が作成または処理する情報で、法律、規則、または政府全体の方針による要求、または特別に許可した、政府機関が保護または頒布をコントロールして取り扱う情報である。CUI は、大統領令（EO:Executive Order）13556、Controlled Unclassified Information（2010 年 11 月）

¹²、32 CFR ¹³のパート 2002、CUI Registry ¹⁴および DoDM 5200.01、Vol 4¹⁵によって確立された、許可なしの開示から保護を必要とするもので、現在更新中である。CUI には、格付け情報や自らシステムを保有・維持している Non エグゼクティブ・ブランチ・エンティティが処理する情報で、エグゼクティブ・ブランチの機関または機関の代理のエンティティからの情報は含まない。レベル 4 で保護される CUI または重要ミッション・データとしての情報の指定は、保有している組織の責任である。CUI とミッション・データによる特定のミッションの適切な影響レベルの決定は、ミッション A0 の責任である。あるタイプの CUI は、DoD PA の特定の条件なしで影響レベル 4 および 5 の CS0 でホストされる資格がない場合がある（例えば、プライバシー）。このレベルは、CNSSI-1253 に基づいて中程度の機密性および中程度の完全性（M-M-x）に基づく CUI 情報分類に対応している。

CUI には、以下を含むがこれらに限定されない多数のカテゴリが含まれる¹⁶。

- ・ 輸出管理対象 - 輸出が合衆国の国家安全保障および非拡散の目的に悪影響を与えると予想される品目、コモディティ、技術、ソフトウェア、またはその他の情報に関する非格付け情報。これにはデュアルユースアイテムが含まれ、輸出管理規則（EAR: Export Administration Regulations）¹⁷、武器規制における国際貨物輸送（ITAR: Traffic in Arms Regulations）¹⁸および軍需品リストで特定された品目、ライセンスアプリケーション、重要な原子力技術情報などが含まれている。

¹² EO 13556: <https://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information>

¹³ Part 2002 of 32 CFR: <https://www.gpo.gov/fdsys/granule/CFR-1998-title32-vol6/CFR-1998-title32-vol6-part2002>

¹⁴ CUI Registry: <https://www.archives.gov/cui/registry/category-list.html>

¹⁵ DoDM 5200.01, Vol 4:
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf

¹⁶ CUI Categories: <http://www.archives.gov/cui/registry/category-list.html>

¹⁷ Department of Commerce EAR:
<https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>

¹⁸ Department of State ITAR:
https://www.pmdtc.state.gov/regulations_laws/itar.html

注：ITAR データは、米国人以外が管理する共有インフラストラクチャ、または 22 CFR 120.17¹⁹および 22 CFR 120.123²⁰で定義されているように輸出許可のない他の組織と一緒に配置することはできない。

- ・ プライバシー情報 - 個人情報、または時として OMB M-07-16²¹で定義された個人を特定可能な情報(PII: personally identifiable information)²²または 18 USC 1028 (d) (7) ²³で定義された識別手段
- ・ 保護された健康情報 (PHI) ²⁴--45 C.F.R. § 160.103) ²⁵で定義されている。
- ・ 明示的な CUI の指定を必要とするその他の情報（例えば、公用に限る、法執行上重要、重要インフラストラクチャ情報、機微なセキュリティ情報）。

レベル 4 の CSO は、米国政府コミュニティまたは DoD だけのコミュニティ（すなわち、CSO は DoD プライベート）をサポートすることができる。

商用レベル 4 の CSP/CSO の顧客には、米国政府のすべての顧客（連邦、州、地方、および部族）およびそれらをサポートする商用顧客が含まれる。場合によっては、レベル 4 の PA は、他の商用エンティティをサポートする CSO に付与することができるが、一般公衆には付与することはできない。

商用レベル 4 の CSO 顧客には以下が含まれる：

- ・ NIPRNet ベースの DoD コンポーネント
- ・ DoD のシステムまたはアプリケーションを運用する DoD の請負業者。これは主に契約の履行のためのものであり、請負業者の CUI/CDI の一般的な保管/処理や請負業者の社内クラウドの使用事例ではない。この場合、請負業者はミッションオーナー

¹⁹ 22 CFR 120.17: <https://www.gpo.gov/fdsys/pkg/CFR-2004-title22-vol1/pdf/CFR-2004-title22-vol1-sec120-17.pdf>

²⁰ 22 CFR 120.-130 International Traffic in Arms Regulations (ITAR) Part 123 - Licenses for the Export of Defense Articles, https://www.pmdtc.state.gov/regulations_laws/itar.html

²¹ OMB M-07-16: <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>

²² NIST SP 800-22, Protecting PII: <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>

²³ USC 1028: <http://www.gpo.gov/fdsys/granule/USCODE-2010-title18/USCODE-2010-title18-partI-chap47-sec1028>

²⁴ PHI: <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/>

²⁵ 45 C.F.R. § 160.103: http://www.ecfr.gov/cgi-bin/text-idx?SID=fdaad816fa8b26001747e9fb198429be&mc=true&node=se45.1.160_1103&rgn=div8

のために運営されているので、CC SRG に明記されているミッションオーナーの要件をすべて満たしている必要がある。

- NIPRNet に接続されているが、分離された COI (Communities of Interest) ミッションパートナーネットワーク。例えば、MedCOI、DREN
- NIPRNet 以外をベースとした DoD コンポーネント。例：売店、教育組織
- 連邦、州、地方、部族政府機関
- DoD 契約者で、DoD CUI または CDI (Covered Defense Information) を DoD 契約の一部として保存/処理する必要があるもの。これは主に契約の履行のためのものであり、請負業者の社内クラウドの使用は該当しない。

レベル 4 の顧客 CSO 接続性：

- NIPRNet ベースの DoD コンポーネントは、DoD が提供し、DoD CIO の承認を受け、NIPRNet の境界、および関連するプライベート接続を介して接続する。
- Non-NIPRNet ベースの DoD コンポーネントは、DoD コンポーネントから提供され、DoD CIO の承認を得て、Non-NIPRNet 境界、および関連するプライベート接続を介して接続する。これ以外の接続方法は、DoD CIO の承認を得なければならない。
- 他のすべての CSO 顧客は、独自の境界とプライベートまたはインターネットベースの接続性を確立する。

DoD NIPRNet から CSO の境界については、セクション 5.10.1、クラウドアクセスポイント (CAP) を参照。

3.2.5 レベル 5：コントロールされた非格付け情報

レベル 5 は、情報所有者、公法、または他の政府規制によって必要とみなされるレベル 4 よりも高いレベルの保護を必要とする CUI に対応している。CUI がこのカテゴリに適合しているかどうかの決定は、情報を分類し、クラウド影響レベルを選択する責任を負っている A0 の判断による。

レベル 5 は、FedRAMP+ C/CE の中に、国家安全保障システム (NSS: National Security Systems) 固有の要件を含めることにより、秘密扱い以外の NSS もサポートしている。この場合、NSS はレベル 5 を実装する必要がある。CUI の内容如何では、DoD PA の特定の容認なしでは影響レベル 4 や 5 の CSO でホストする資格がない場合がある（例えば、プライバシーのため）。このレベルは、CNSSI-1253 に基づいて中程度の機密性と中程度の完全性 (M-M-x) に基づく NSS および CUI 情報の分類に対応する。

レベル 5 の CSO は、連邦政府コミュニティまたは DoD だけのコミュニティをサポートすることができる（すなわち、CSO が DoD プライベート）。

商用レベル 5 の CSP/CSO の顧客には、すべての連邦政府の顧客（連邦機関のみ）を含み、これには DoD コンポーネントや DoD のために DoD システムを運用している DoD 請負業者が含まれている。

商用レベル 5 の CSO 顧客には以下が含まれる：

- NIPRNet ベースの DoD コンポーネント
- NIPRNet に接続されているが、分離された COI ミッションパートナーネットワーク。例えば、MedCOI、DREN
- NIPRNet 以外をベースとした DoD コンポーネント。例：売店、教育組織
- 非格付け NSS を運用する連邦政府機関
- DoD のためにシステムやアプリケーション（NSS の秘密区分なしを含む）を運用している DoD の請負業者。これは主に契約の履行のためのものであり、請負業者の社内クラウドの使用は該当しない。この場合、請負業者はミッションオーナーのために運営されており、CC SRG に明記されているミッションオーナーの要件をすべて満たしている必要がある。

レベル 5 の顧客 CSO 接続性：

- NIPRNet ベースの DoD コンポーネントは、DoD が提供し、DoD CIO の承認を得て、NIPRNet の境界、および関連するプライベート接続を介して接続する。
- NIPRNet 以外をベースとした DoD コンポーネントは、提供された DoD コンポーネントを介し、DoD CIO の承認を得て、NON-NIPRNet 境界、および関連するプライベート接続を介して接続する。これ以外の接続方法は、DoD CIO の承認を得なければならない。
- 他のすべての CSO 顧客は、独自の境界とプライベートまたはインターネットベースの接続を確立する。

DoD NIPRNet から CSO の境界については、セクション 5.10.1、クラウドアクセスポイント（CAP）を参照。

3.2.6 レベル 6 : SECRET までの格付け情報

レベル 6 は、(i) E013292²⁶で改正された E012958: *Classified National Security Information* (April 17, 1995) または、これに先立つ指令、国家安全保障情報、または (ii) P.L. 83-703²⁷で改正された原子力エネルギー法 1954 による秘密データ (RD: Restricted Data) を収容する。この時点では、該当する E0 に従い、SECRET 以下に分類された情報のみが、このレベルでホストされることが許可されている。このレベルは、中程度の機密性と中程度の完全性 (M-M-x) までの格付け情報に対応している。

レベル 6 の CSO は、連邦政府コミュニティまたは DoD のみのコミュニティをサポートすることができる (すなわち、CSO は DoD プライベート)。CSO インフラストラクチャ全体が専用で、他の CSP/CSO インフラストラクチャとは分離されていることが要求されているため、レベルの 6 CSO は、DoD または連邦機関との契約による CSP によってのみ提供される。この意味で CSO は「商用」とはみなされない。

レベル 6 の CSO 顧客には以下が含まれる：

- SIPRNet ベースの DoD コンポーネントと連邦機関
- SIPRNet に接続されているが、COI ミッションパートナーの SECRET ネットワークとは分離した連邦政府の SECRET ネットワーク
- DoD のために SECRET NSS を運用している DoD の請負業者。これは主に NSS 契約の履行のためであるが、契約者の SECRET CDI の一般的な保管/処理のために (承認されていれば) 使用することもできる。

CSO へのアクセスは、1 つまたは複数のプライベート SIPRNet 接続を介して行われる。

第 4 章 クラウドサービス提供のリスクアセスメント

物理的にオンプレミスのシステムやアプリケーションを前提にしたシステムからクラウドコンピューティングへ移行するには、商用 CSO の使用に対応するために、DoD リスク管理プロセスを微調整する必要がある。目標とするところは、DoD RMF に沿って DoD のコアミッションとネットワークのセキュリティを保証しながら、セキュリティ要件とコントロールを、クラウド内の DoD 情報の重要度に対応し、費用対効果に優れた効率的な方法で対処することである。DoD は、ミッションとクラウドの関係をサポートするため、クラウド環境で動作するデータの重要性和機密性、ミッションに広く対応する情報影響レベル (3.2 「情報影

²⁶ E0 12958 as amended by E0 13292: <http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html>

²⁷ AEA 1954 as amended: <http://pbadupws.nrc.gov/docs/ML1327/ML13274A489.pdf#page=23>

響レベル」で説明)を定義している。DoD PA のリスクアセスメントプロセスは、CSP の CS0 がサポートできる影響レベルの要件を評価することに重点を置いている。CSP の CS0 を選択する場合、ミッションオーナーは、運用上の要求に適合し、CS0 に処理または保存される情報の分類に対応した情報影響レベルで DoD PA を保持している CS0 を選択する必要がある。クラウド内で運用されているミッションシステムに必要な ATO を付与する際に、ミッションオーナーの認可当局が PA とそのサポート文書を活用する必要がある。

注：CC SRG の目的上、「アセスメントと認可 (A&A: Assessment and Authorization)」という用語の使用は、「セキュリティ管理策アセスメント、リスクアセスメント (セキュリティ管理策アセスメントによって通知)、継続的アセスメント(継続的な監視)、およびシステム認証」など、一連の RMF プロセスを含む。

4.1 商用/Non-DoD のクラウドサービスのアセスメント

2014 年 12 月 15 日の商業用クラウド・コンピューティング・サービスの取得および使用についてのガイダンスに関する DoD CIO メモで、「コンポーネントは、FedRAMP が承認したクラウドサービスで、**公開された**秘密区分以外の DoD 情報をホストする可能性」について述べている。このメモはまた、「FedRAMP はすべての DoD クラウドサービスの最低限のセキュリティ基準」であると述べている。

影響レベル 2：セクション 3.2 で概説した定義を使用すると、影響レベル 2 の情報は、政府が中程度のレベルで FedRAMP に準拠していると評価された CSP でホストされる。許容される 2 つの政府のアセスメントは次を含む。

- JAB PA - 連邦政府全体にとって、存在するリスクは許容できるレベルにあるとの JAB の決定に基づく。DoD は、JAB PA セキュリティアセスメント成果物の技術レビューに積極的に参加している。
- 機関の ATO にリストされた FedRAMP - CSP が FedRAMP の認定/承認された 3PAO によって評価されたアセスメントと連邦政府機関によって発行された ATO に基づく。

DoD は、DoD PA を授与されて DoD クラウドサービスカタログ²⁸に掲載される前に、追加の NIST 800-53 RMF コントロールアセスメントをレベル 2 では実行しない。

²⁸ DoD Cloud Service Catalog:<https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Approved-Commercial.aspx> (DoD CAC/PKI required)
<http://www.disa.mil/~media/Files/DISA/Services/Cloud-Broker/AuthorizedCloudServicesCatalog.pdf> (Public)

影響レベル 4/5：影響レベル 4 以上の RMF アセスメントは、FedRAMP 中または高ベースラインのセキュリティ管理策と 5.1.2 「DoD FedRAMP+セキュリティ管理策/強化」に記載されている DoD 固有のコントロール/要件の組み合わせと、この SRG 全体のその他の要件に基づいている。可能ならば、DoD は前の FedRAMP-JAB または FedRAMP セキュア・リポジトリおよび CPS から提供された追加の CPS 固有の成果物の中の Non-DoD の機関の認可からの文書・成果物を利用する。FedRAMP+要件は、FedRAMP の認定/承認された 3PAO によって評価される。リスクの全体的な決定は、DoD PA の決定をサポートする DISA クラウドセキュリティ管理策アシスタント (SCA) 組織によって準備される。DISA A0 (旧 DISA DAA) が DoD PA を承認する。

レベル 4 / 5 DoD PA の CSP の評価と、その後の DoD の要員が利用できる DoD クラウドサービスカタログ²⁹への掲載には、3つの方法がある。これらは：

- **FedRAMP JAB PA または JAB PA 取得中の CSP：**DoD は、FedRAMP プロセスの一部として作成されたドキュメンテーション・成果物と、FedRAMP 影響レベル 4 以上では言及されない DoD 固有のセキュリティ管理策のアセスメントを補完として活用する。FedRAMP JAB PA を有する CSP は、認定/承認された 3PAO によって FedRAMP M 中または高ベースラインに対して評価されたものである。DoD は、JAB PA を取得する過程で、費用を最小限に抑え、アセスメントプロセスの効率を高めるために、並行した (FedRAMP と FedRAMP +) 活用を推奨している。

注：DoD SCA と DoD CIO は既にアセスメントと認可アクティビティに関わっていることから、DoD にとって好ましい DoD PA の取得方法である。

- **FedRAMP に掲載された Non-DoD の機関 ATO：**認定/承認された 3PAO によって評価されたセキュリティ管理策に基づく Non-DoD の機関の認可を受けた CSP は、認可が受け入れられて FedRAMP 機関の認可に記載されていれば DoD PA として評価される。許容される最小基準は FedRAMP 中程度である。Non-DoD 機関からの ATO の情報は、DoD 固有のコントロールと要件によるアセスメントで補足される。この追加のアセスメントは、CSP の 3PAO によって実施され、PA の獲得に向けた DISA SCA のレビューのために提出されるべきである。

²⁹ DoD Cloud Service Catalog:

<https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Approved-Commercial.aspx>
(DoD CAC/PKI required)

<http://www.disa.mil/~media/Files/DISA/Services/Cloud-Broker/AuthorizedCloudServicesCatalog.pdf> (Public)

注：ミッションオーナー、AO や DISA SCA は、DoD 以外の機関では DoD には相応しくないリスクを受け入れている可能性があるため、当該機関 ATO を慎重に評価する必要がある。

- **DoD コンポーネントが評価した PA:** CSP の CSO が FedRAMP PMO とは独立して、FedRAMP の認定/承認された 3PAO (強く推奨)、DISA クラウド SCA 組織、または DISA SCA クラウド組織と連携したその他の承認された DoD SCA 組織**により、完全に評価されたもの。CSP の CSO は、FedRAMP 中 (または高) ベースラインと FedRAMP+要件の両方に対して評価されなければならない。

FedRAMP PA や 3PAO がアセスメントした Non-DoD 機関の ATO が存在しない場合、CSP の CSO の DoD コンポーネントアセスメントは、以下の 2 つの状況下でのみ行われる可能性がある。:

1. DoD 組織が、特定の CSP の CSO のみが認可の要求を成し遂げることができるような、検証されたミッション要求を持っている場合
2. DoD 組織が CSP として活動し、CSO を開発してインスタンス化する場合

CSP の CSO が承認される必要がある DoD の組織は、DISA クラウドセキュリティアセスメントチームと協力して、アセスメントのためのリソースをサポートする必要がある。FedRAMP、FedRAMP+セキュリティ管理策、およびその他の SRG 要件に関するこのアセスメントにより、DoD PA と適切な影響レベルを付与するかどうかを決定する。

CSP が DoD で評価された PA を取得し、提供するサービスが他の連邦機関によって活用される場合、CSP のアセスメントパッケージは FedRAMP のセキュア・リポジトリと DoD クラウドサービスカタログと共有され、利用可能となる。サービスの提供が DoD の顧客のみに提供される場合、CSP のアセスメントパッケージは、プライベートクラウドが FedRAMP カタログに含まれないため、DoD クラウドサービスカタログでのみ利用可能である。

DoD の CSP IaaS/PaaS/SaaS CSO は DoD RMF の下で全ての ATO について評価され、DISN との接続許可のサポートを行うが、同様に DoD CSP IaaS/PaaS CSO は、この SRG における商用 CSP の要求に従って PA が評価される。DoD CSP IaaS / PaaS CSO の PA 獲得によって、ミッションオーナーの AO は、商用の CSP が CSO 上にシステムやアプリケーションを構築するための ATO の授与と同じように PA を活用することができる。DoD SaaS CSO のアセスメント情報については、第 4.2 項「DoD クラウドサービスのアセスメント」を参照。

**「その他の承認された DoD SCA 組織」には、コンポーネントの AO をサポートするセキュリティ管理策アセスメント活動を日常的に実行する DoD コンポーネントレベルの組織が含まれる。例としては、DISA のリスク・マネジメント・エグゼクティブ (RME) アセスメントおよび評価部 (Certification and Assessment Division) RE5、海軍の宇宙海軍システム指令部 (SPAWAR: Navy's Space and Naval Warfare Systems Command) および空軍宇宙司令部 (AFSPC: Air Force Space Command) がある。

CSO は同じ 3PAO によって FedRAMP と DoD の両方の要件を同時にアセスメントしていても良い (そうすべき)。これにより、CSP は、FedRAMP と DoD クラウドカタログの両方に CSO を含めることを検討している場合に、アセスメントの重複を避けることができる。

プライマリ CSP であるか CSO が構築された基盤となっている CSP であるかに関わらず、CSP に関する所有権の変更は、DoD PA の継続に関連した影響とリスクを DISA AO によって審査されなければならない。さらに、DoD CIO、DISA AO やミッションオーナーは、CSP の所有権に変更が予想される場合は、PA のレビューを可能とし、必要であればミッションオーナーが CSP から情報やデータを外して取得できるよう、変更が発生する 6 ヶ月前までに通知を受ける必要がある。ミッションオーナーは、SLA/契約の CSP 所有権に対応する必要がある。DoD の主な懸念事項は、米国外の組織への販売である。

4.3.3 「ミッションリスク」で言及されるように、DoD PA を持つ CSO による CSO を使った申請に関して、運用開始前に ATO (または IATT) を得る要件を省略するものではない。

注意: DoD Cloud SCA 組織は NIST SP 800-53 C/CE のアセスメントを熟知していなければならない。クラウド SCA 組織全般のアセスメントの品質及び全ての DoD コンポーネントやミッションオーナーが利用する DoD の PA の品質を標準化するために、DoD SCA 組織は、American Association for Laboratory Accreditation (A2LA³⁰) で認証されるべきであり、FedRAMP により 3PAO³¹ として承認されるべきである。あるいは、DoD PA のために活用されるすべてのアセスメントは、FedRAMP が承認した 3PAO によって行われなければならない。さらに DoD PA は RMF に基づくものであり、DoDI 8500.2 IA コントロールを用いた旧式の DoD の情報保証認証および認定プロセス (DIACAP: DoD Information Assurance Certification and Accreditation Process) の下でアセスメントされた CSP/CSO は、PA の基盤である標準化を破り、その品質を損なうことになるため DoD PA の資格を持たない。

³⁰ A2LA: <http://www.a2la.org/appsweb/fedramp.cfm>

³¹ FedRAMP 3PAO approval: <https://www.fedramp.gov/participate/3paos/>

影響レベル 6：格付け情報（すなわち、Non-DoD で商用 CSP およびレベル 6 の CSO）を処理、保管、送信するオフプレミスの DoD 請負施設および情報システムのアセスメントと認可は、国家産業安全保障プログラム（NISP: National Industrial Security Program）（Executive Order 12829³²で定義されている）と連邦規則 48 コード（CFR:Code of Federal Regulations）サブパート 4.4-業界内³³の格付け情報の保護に従った産業セキュリティ規則（ISR:Industrial Security Regulation）（DoD 5220.22-R）³⁴及び国家産業安全プログラム（FAR:Federal Acquisition Regulations）52.204-2 - セキュリティ要件³⁵と併せて実施されなければならない。NISP の方針は、アメリカ国防情報局（OUSD (I)）の産業セキュリティ部門と、DoD の防衛セキュリティサービス（DSS:Defense Security Service）の権限である。DoDI 5220.22³⁶は、E.O. 10865 と 12829 に従った NISP の管理の責任を DoD へ付与し、業界へ開示された格付け情報が適切に保護されていることを確実にしている。DoD コンポーネントに対する NISP の責任は、DoD 5220.22-R および DoDI 5220.22 で示され、レベル 6 を提供する商用 CSP は国家産業安全保障プログラム運用マニュアル（DoD 5220.22-M）³⁷を遵守しなければならない。ISR、NISPOM、指定承認機関（ODAA: Office of the Designated Approving Authority）のプロセスマニュアル³⁸[39]とともにガイダンスを提供している。

注：DoD CIO は、すべての CSP と CSO が DoDI 8510.01- DoD RMF 及び CNSSI 1253-セキュリティ分類及び国家のセキュリティシステム及び CC SRG で定義された同じ一連の要件とサイバーセキュリティ管理策のベースラインによって評価されることを意図している。影響レベル 6 に関するオフプレミスの商用 CSP 及びその CSO の承認をサポートする要件とプロセスは、OUSD(I) 及び NISP ポリシーとして DSS と調整され、手順は更新される。DoD レベル 6 の仮承認のための、オフプレミス CSP およびその CSO に対する更新されたガイダンスと要件は、CC SRG の将来のリリースに反映される可能性がある。

4.2 DoD クラウドサービスとエンタープライズサービスアプリケーションのアセスメント

DoD が運用する CSO（例：milCloud IaaS/PaaS）は、この SRG の記載と同じ要件及び商用 CSO と同じセキュリティ管理策の対象である。しかし、DoD CSP/CSO のプログラムとサービ

³² EO 12829, NISP: <http://www.archives.gov/isoo/policy-documents/eo-12829.html>

³³ 48 CFR Subpart 4.4:

<https://www.gpo.gov/fdsys/granule/CFR-2011-title48-vol1/CFR-2011-title48-vol1-part4-subpart4-4>

³⁴ DoD 5220.22-R: <http://www.dtic.mil/whs/directives/corres/pdf/522022r.pdf>

³⁵ <https://www.gpo.gov/fdsys/pkg/CFR-2002-title48-vol2/pdf/CFR-2002-title48-vol2-sec52-204-1.pdf>

³⁶ DoDI 5220.22 NISP: <http://www.dtic.mil/whs/directives/corres/pdf/522022p.pdf>

³⁷ DoD 5220.22-M, NISPOM: <http://www.dss.mil/documents/odaa/nispom2006-5220.pdf>

³⁸ ODAA) Process Manual: <http://www.dss.mil/documents/odaa/ODAA%20Process%20Manual%20Version%203.2.pdf>

スは、サービスの情報分類に相応する CNSSI 1253 に列挙されている一連のコントロールおよびコントロール強化に基づいた DoD 8510.01 に従った、DoD リスク管理手順に従わなければならない。これは、DoD CSO が適切な FedRAMP ベースライン（最小限は中程度）と適切な CNSSI 1253 ベースライン（調整済み）からなる総ベースラインに対して評価されなければならないことを意味する。DoD CSO は、PA の代わりに利用できる完全な ATO を必要とするか、またはミッションオーナーとその AO によって活用される PA を生成する必要がある。

SaaS モデル（例えば、DEE (Defense Enterprise Email)、DCS (Defense Collaboration Service)、DoD Enterprise Portal サービス (DEPS)) の下でクラウドサービスと見なされる DoD エンタープライズサービスプログラムは、DoDI 8510.01 要件と CNSSI 1253 のベースラインの対象である。そのようなプログラムは、前述のように DoD で評価されたものであり、FedRAMP プログラムを通じた評価ではないので、DoD ATO を FedRAMP のセキュア・リポジトリとは共有しない。

DoD は DoD の情報保証認証および認定プロセス (DIACAP) から DoD RMF に移行しつつある。DIACAP は、NIST SP 800-53 セキュリティ管理策カタログではなく、DoD で定義された一連のセキュリティ管理策に基づいている。DIACAP の下で開始され承認されたクラウドサービスは、DoD 8510.01 に定義されている DoD 移行ガイダンスまたは補足的な DoD ガイダンスに従って、RMF を使用して評価され承認される。

影響レベル 6： オンプレミスでレベル 6 の CSO（すなわち、DoD または DoD の請負業者が DoD データセンターで CSO を管理）のアセスメントと認可は、DoD が決めた方針とプロセスに従い、DoD の格付け施設、アプリケーション、接続許可、DoD 及び DoD 請負業者のクリアランスに対する DoD RMF に従って、DoD コンポーネントの SCA により、他の SIPRNet 区画、サービスまたはアプリケーションと同じように実施される。この A&A と併せて、CSO が認可コンポーネント以外の DoD コンポーネントに提供され、CSO がすべての CSO についてこの CC SRG で定義された基準を満たしている場合、この CSO は DoD PA を得ることができる。オンプレミス CSO が商用 CSP または他の DoD 請負業者によって運営/管理される場合、CSP/請負業者は格付け情報を扱う DoD 請負業者の場合のように適切な施設のクリアランスと要員のクリアランスを要求される。請負業者のクリアランスに関する詳細はよく知られているので、CC SRG の範囲外である。

DoD PA を得るには、DoD オンプレミスで影響レベル 6 の CSO は、少なくとも FedRAMP または高ベースライン、レベル 6 FedRAMP+ C/CE および CNSSI 1253 付録 F、付録 5 の格付け情報オーバーレイ C/CE で評価されるようになる。そのような CSO は、CSO で処理/保存される情報の分類に関連するベースラインで追加の CNSSI 1253 C/CE を満たす必要がある。

注記：オンプレミス請負業者が管理する CSO の組織施設と要員のクリアランスに関する追加要件については、セクション 5.6.2.2、CSP 要員の要件 - PS-3：レベル 6 トピックの背景調査を参照。

4.3 クラウドサービスの提供とミッションオーナーのリスク管理

リスク管理では、CSO とサポートされるミッション（ミッションオーナーのシステムまたはアプリケーション）の両方を考慮する必要がある。各 CSO は DoD ミッションシステムをホストするために DoD PA を付与されなければならない。PA とサポート文書は、CSP によって提供されるコントロールの相互主義の基礎として、ミッションオーナーのリスク管理担当者によって使用される。コントロールはサービスモデル（IaaS、PaaS、SaaS）毎に異なり、プライバシーや分類管理などの要件にも影響を受ける。さらに、CSO とミッションオーナーの両方が要件を満たす必要がある「共有コントロール」が存在する。責任ある AO は、運用許可を与える際に、ミッションオーナーの責任内のアセスメント・リスクで補完された PA 情報を活用する。

この SRG で定義されているように、DoD クラウドセキュリティ要件の実装にあたり、CSO によって提供され対処されるものと、ミッションオーナーによって対処されるものの違いを理解することが重要である。

4.3.1 クラウドコンピューティング、認可の境界

クラウドコンピューティングには、2つの主要な認可境界が存在する。これらは、一般に CSP とミッションオーナーの間のコントロールの区分けによって決定される。（図 2 - 「セキュリティ継承とリスクの概念的区分」を参照）、一般に次のように定義されている。

1. FedRAMP と DoD PA が扱う CSP および CSO 認可境界は 2つの部分で構成されている：
 - a. CSP 組織、その運用/セキュリティ方針と手順、物理的設備、ネットワーク、ハードウェア・サーバ・プラットフォーム、ハイパーバイザ、VM、アプリケーションなど、企業ネットワークにサービスを提供し、間接的に CSO をサポート。CSO は、C/CE がどの程度うまく実装されているかに基づく残存リスクに沿った CSP の実装による C/CE を継承。
 - b. CSO には、CSO を直接サポートするインフラストラクチャと、サービスのタイプごとに以下が含まれる。
 - IaaS：IaaS サービスを提供するネットワーク、ストレージ、コンピューティングプラットフォーム、ハイパーバイザを含む。

- PaaS : IaaS で使用されるデバイスやプラットフォーム、または構築物をベースに構築し、VM、OS やプラットフォームアプリケーションが含まれる。CSP が OS やプラットフォームアプリケーションを管理/保護する場合、これらの一部またはすべてと IaaS にリストされているものがこの認可境界に含まれる。

注：一部の PaaS サービスは仮想化を使用していない可能性があり、サービスによって提供されるプラットフォームアプリケーションがゼロから構築される可能性がある。これは、NIST のクラウドサービスの定義と一致しない。

- SaaS : IaaS や PaaS で使用されるデバイス、プラットフォーム、アプリケーション、または構築物をベースにして、CSP のサービス提供を構成する最終的なアプリケーションとそれをサポートするすべてのアプリケーションを含むことができる。IaaS や PaaS に記載されているこれらの一部または全部が、この SaaS 認可境界に含まれている。

注：一部の SaaS サービスは仮想化を使用していない可能性があり、サービスによって提供されるアプリケーションがゼロから構築される可能性がある。これは、NIST のクラウドサービスの定義と一致しない。

2. ミッションオーナーの ATO に言及されるミッションオーナーのシステム/アプリケーションの認可境界。ミッションオーナーのシステム/アプリケーションは、C/CE がどの程度うまく実装されているかに基づく残存リスクに沿って、CSP が組織と CSO へ実装する C/CE を継承する。ミッションオーナーの ATO は、これらの継承された C/CE とともに、以下をベースとしたサービスタイプを含んでいる。

- IaaS : ミッションオーナーが運用/維持する、OS、アプリケーションと関連するデータストレージと共に、仮想ネットワークと VM のシステム。
- PaaS : 仮想ネットワークと VM のシステムの一部で、ミッションオーナーが管理する OS、プラットフォームアプリケーション、関連データストレージと CSO の上に実装されたミッションオーナーによるアプリケーション。
- SaaS : ミッションオーナーが管理する CSO の一部（ユーザカウントなど）と、CSO とミッションオーナーが CSO とクラウドの使用に関連する DoD セキュリティポリシーに準拠するためのミッションオーナーポリシーと手順。

すべてのサービスタイプ：ミッションオーナーが使用する転送中のデータ暗号化方式、ユーザと管理のためのサービスへのアクセスのためにミッションオーナーによって実装され

る追加のアクセス制御レイヤー、顧客が実装または管理する暗号化された保管データ、その他の DoD 要件は、CSP の顧客に適合しなければならない。

4.3.2 クラウドサービスの提供 (CS0) のリスク

DoD PA は、適正な DoD のセキュリティ要件に対する CS0 の暫定的または部分的な許容リスクの決定を提供する。DoD PA のアセスメントプロセスは、サポートされている影響レベルに対応して CS0 のリスクを評価し提示を行う。レベル 4 以上では、DoD PA 評価プロセスにおいて、CSP が DoD ネットワークへの接続を許可する DoD のリスクも評価されることを認識することが重要である。

4.3.3 ミッションリスク

ミッションとは、DoD エンティティが CS0 を取得または使用する情報システムと機能を指す。これは、IT 対応ミッションの実施における SaaS CS0 の直接使用、または IaaS/PaaS CS0 上の IT システムまたはアプリケーションのインスタンス化である。

ミッションオーナーが使用するすべての DoD または Non-DoD の CS0 には、DISA によって DoD PA が発行されている必要がある。包括的なミッションリスクは、ATO の発行を通じ、ミッションオーナーの AO によって評価・認可が継続される。ミッションオーナーのシステム/アプリケーション/クラウドのユースケースは、コンポーネントの AO またはミッションオーナーのシステム/アプリケーション/クラウドのユースケースのリスク受諾に直接責任を持つ他のコンポーネントに認定された下位の AO によって ATO が発行されなければならない。これは、すべての情報影響レベルに適用される。このミッションシステムの ATO 要件は、DoD CSP IaaS/PaaS CS0 にまで拡張され、その ATO は、CS0 上に構築された場合、完全なミッションシステム/アプリケーションのリスクに対応できないため、DISN への接続のみを許可する。

ミッションオーナーが DoD PA を持つ CS0 のみを使用するという要件は、CSP/CS0 のサードパーティ請負業者または再販業者によって提供される CS0 にも及ぶ。DoD で使用するためのソリューションに統合されているか、または DoD エンティティに再販されている CS0 はすべて、DoD PA が必要である。

ミッションオーナーは、DoDI 8510.01 で定義されたプロセスに従って、ミッションシステムやアプリケーションを分類する。次に、ミッションオーナーは、DoD クラウドサービスカタログから、セキュリティの体制とミッションオーナーとその AO のリスク許容度に基づいて CS0 を選択する。CS0 は評価され、利用のために暫定的に認可されるが、ミッションオ

オーナーは、指定された AO から運用許可 (ATO) を取得するために RMF に従って進めなければならない。

ミッションオーナーは、CSP が満たして維持しているセキュリティ管理策（またはその一部）について、CSO からのコンプライアンスを継承する。IaaS または PaaS オファリングで構築されたミッションオーナーのシステムまたはアプリケーションは、システム/アプリケーション内の同じセキュリティ管理策の多くを満たすことになる。SaaS 製品を契約しているミッションオーナーは、CSO からセキュリティ管理策の大部分を継承している。継承は、特定のサービスモデル内で動作する CSP 間で異なるため、個別に評価する必要がある。また、高い影響レベルや、オーバーレイ制御（例えば、プライバシー）が増えると、コントロールの数が増えることにも留意されたい。図 2 は、CSP とミッションオーナーの間で共有される管理と責任の分担とともに継承の概念を示す。

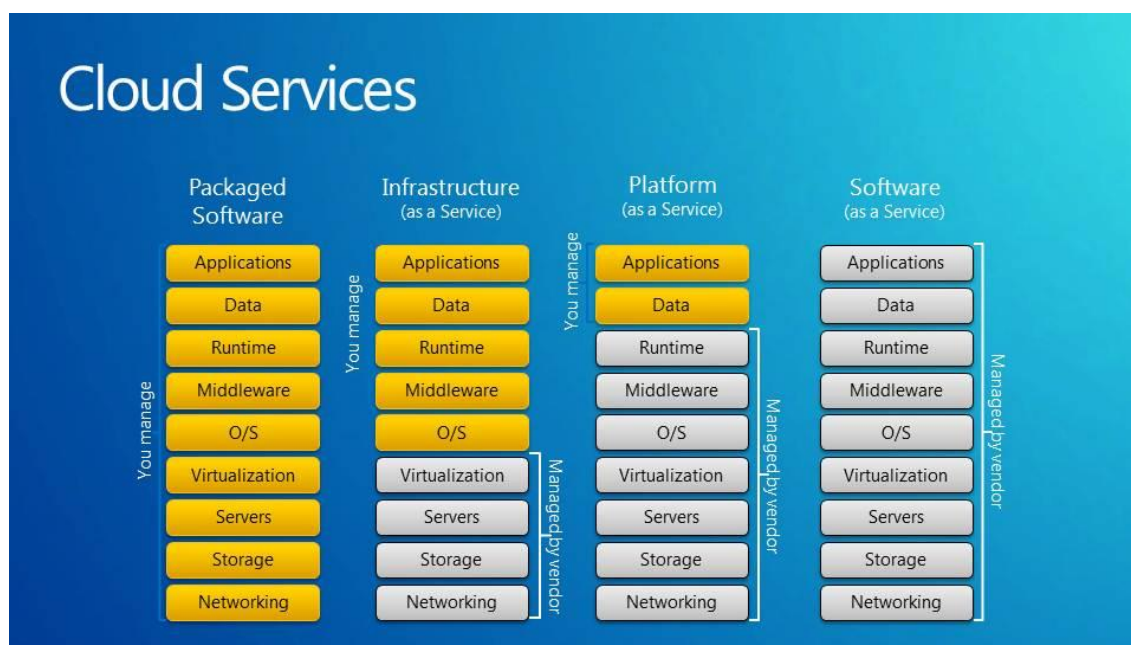


図 2 セキュリティ継承とリスクの概念的区分³⁹

暫定的に認可された CSO から始めることの利点は、セキュリティ管理策のアセスメント作業の多くが既に達成されていることにある。ミッションオーナーとその AO は、ミッションシステム/アプリケーションに選ばれた CSO を利用する際に、ミッションが継承するリスクを理解するために、FedRAMP と DoD PA の資料を検討する必要がある。ミッションオーナーは、ATO を取得する前に、容認できないと考えられるリスクを補うコントロールを実装するか、CSP へ実装を要求することがある。追加のコントロールは、ミッションオーナーの SLA/CSP との契約に反映されなければならない。

³⁹ Figure 2: Graphic courtesy of Microsoft

4.4 CSM v2.1 から CC SRG v1r1 への CSP 移行およびその後の更新

FedRAMP は、NIST SP 800-53 rev3 に基づく FedRAMP v1 ベースラインから NIST SP 800-53 rev4 に基づく FedRAMP v2 ベースラインへ CSP アセスメントを移行する移行戦略⁴⁰を提供している。この戦略は、2014 年 6 月 6 日に発効した。重要なポイントは次のとおりである。

- 2014 年 6 月 1 日以降に開始される新しいアセスメントは、直ちに NIST SP 800-53 rev4 に基づく FedRAMP v2 ベースラインへ移行
- 2014 年 6 月 1 日より前の NIST SP 800-53 rev3 に基づく FedRAMP v1 ベースラインに対して評価済の CSP は、このコースで継続するが、認定日の 1 年以内に FedRAMP v2 ベースラインに移行する必要がある。
- 現在継続モニタリングの CSP は、FedRAMP v2 ベースラインへの移行を次年のアセスメントまでに完了しなければならない。

注：元の移行計画に従って、FedRAMP は 2015 年 9 月 9 日に移行計画を次のように更新⁴¹した。

「FedRAMP は、すべての CSP が 2015 暦年の終わりまでに FedRAMP 改訂 4 の要件に移行することを要求している。2016 年 1 月 1 日現在、FedRAMP PMO は Revision 3 のシステム文書を FedRAMP 準拠としては受け付けない。」

この SRG の要件は、最終的な公開直後に有効になる。しかし、CSP アセスメントの DoD 移行計画は、FedRAMP 計画を次のように反映する予定である。

- この CC SRG のリリース後に開始される新しいアセスメントは、これらの要件に対して評価される。
- 現在 CSM v2.1 の要件に照らして評価されている CSP はこのコースで継続するが、次回の FedRAMP/DoD 年次アセスメントと連携して CC SRG 要件に準拠する必要がある。
- 現在 CSM v2.1 で継続モニタリングされている CSP は、次年の FedRAMP/DoD アセスメントまでに CC SRG コントロール要件へ移行を完了しなければならない。

⁴⁰ FedRAMP transition strategy: www.fedramp.gov/files/2015/03/FedRAMP-Revision-4-Transition-Guide-v1.0-1.docx

<https://www.fedramp.gov/files/2015/01/FedRAMP-Rev-4-Transition-Additional-Guidance.docx>

⁴¹ FedRAMP transition strategy 9/2015: <https://www.fedramp.gov/files/2015/01/FedRAMP-Rev-4-Transition-Guide-v3-0.pdf>

CSM v2.1 を使用し、FedRAMP v1 に基づく CSP のために発給された DoD PA は、前述のタイムライン内でコンプライアンスが達成されている限り、DoD PA の期間中有効である（取り消されない限り）。CSO を活用している DoD ミッションオーナーのシステムでは、FedRAMP v2 または新しい FedRAMP+セキュリティ管理策に基づくリスクがまだ評価されていない期間が発生する可能性がある。ミッションオーナーとその AO は、CSP が準拠を要求されるか、SLA/契約の中に必要な準拠を含むまでの間、リスクを受容可能か否か判断するために、コントロールをレビューしなければならない。

注：早期移行を CSP が希望する場合は、いつでも移行可能である。

注意：CC SRG における FedRAMP v2 という用語、Rev 3 から NIST SP 800-53 rev4 に更新された FedRAMP ベースラインを指す。これは FedRAMP 2.0 と指定される未完成の FedRAMP 改訂版と混同しないこと。

4.4.1 CC SRG バージョン/リリースから更新された CC SRG バージョン/リリースへの CSP 移行

CC SRG 更新の要件は、メジャーバージョンの更新かマイナーリリースの更新かにかかわらず、最終的な公開直後に有効となる。しかしながら：

- CC SRG アップデートのリリース後に開始される新しい CSP/CSO アセスメントは、更新された要件に対して評価される。
- 以前の CC SRG の要件に照らして評価されている CSP/CSO はこのトラックで継続するが、次の FedRAMP/DoD の年次アセスメントと連携して現在の CC SRG の更新に移行する必要がある。すなわち、PA の獲得から 1 年である。
- 以前の CC SRG の下で、継続モニタリング中の CSP/CSO は、現行の CC SRG 要件にできるだけ早く対応するために 30 日以内に行動計画とマイルストーン（POA&M: Plan of Action and Milestones）を提供することになるが、遅くとも次の FedRAMP/DoD 年次アセスメントまでが期限で、CC SRG の更新がリリースされてから 6 ヶ月後に予定されていれば 1 年を超えることはなく、つまり、移行は可及的速やかであって、6 ヶ月～1 年を超えることはない。

以前の CC SRG を使用し、FedRAMP v2 に基づく CSP のために発行された DoD PA は、上記のタイムラインでコンプライアンスが達成されている限り、DoD PA の期間中有効である（取り消されない限り）。移行の期間に、CSO を活用する DoD ミッションシステムは、現在の CC SRG セキュリティ管理策に基づくリスクがまだ評価されていない期間が発生する可能性がある。ミッションオーナーとその AO は、CSP が対応に応じるか、または SLA/

契約の中に要求された対応を含むかどうかを決定するまでに、リスクが許容可能かどうかを判断するためにコントロールをレビューする必要がある。

注：早期移行を CSP が希望する場合は、いつでも移行可能である。

4.5 RFP への応募と契約獲得に関連した DoD PA ; DFARS の解釈

このセクションでは、契約獲得に関連する PA および ATO に関する情報を提供している。以下は、現在、DoD 調達規定補足 (DFARS: Defense Federal Acquisition Regulation Supplement) で定義されている、または将来定義される契約条項を変更するものではなく、主にオンプレミス CSO に関し、追加の明確化の情報を提供している。

このトピックは、2つの観点を対象としなければならない。これらは：

1. 商用 CSO インフラストラクチャがオフプレミスの場合（典型的には、既に存在している場合）、vs
2. CSO インフラストラクチャが物理的または仮想的にオンプレミスで契約されている場合（典型的には、専用ハードウェアを使用して構築する必要がある場合）

オフプレミス商用サービス：DFARS SUBPART 239.76-CLOUD COMPUTING、⁴²239.7602-1 に従って、CSP は、契約受注の前に適切なインフォメーション・影響レベル（IIL: Information Impact Level）で DoD PA を持っていなければならない。本質的にこれは、DoD クラウドサービスの RFP に応える前に CSP/CSO が通常 DoD PA を持っていなければならないことを意味する。

これは、RFP に応える CSP/CSO のインテグレータとリセラーにまで及ぶ。DoD で使用するソリューションに統合されているか、DoD エンティティに再販されている CSO は、該当する IIL における DoD PA を必要とする。

DFARS 239.7602-1 には2つの例外がある：

1. 要件を DoD CIO が免除
2. クラウド・コンピューティング・サービスの要件が、米国政府の施設から提供されるプライベートの**オンプレミス**版用である場合。このような状況下では、クラウドサービスプロバイダは運用上の使用に先立って暫定的な認証を取得する必要がある。これは以下で明確化される。

⁴² DFARS SUBPART 239.76:
http://www.acq.osd.mil/dpap/dars/dfars/html/current/239_76.htm#239.76

さらに、ミッションオーナーが商用オフプレミスの CSO とその PA を活用する場合、ミッションオーナーの AO は、DoD RMF ポリシーを満たすために CSO を使用するための ATO を提供する。これは、DoD CIO のクラウドメモにも記載されている。

オンプレミス（物理的または仮想的）：一般的な DFARS ルールはオンプレミス CSO に適用されるが、CSP の CSO の商用インスタンス化が評価されて DoD PA を得ることは DoD にとって有益である。これによって、商用のサービスとインフラが、適切な IIL において DoD の情報をホストすることが可能であるが、この PA は、CSO による別のオンプレミス・インスタンス化では直接利用することはできない。

あるオンプレミス CSO は、CC SRG の他の章で説明されているように、DISN サービス（すなわち、NIPRNet または SIPRNet）に接続される DoD プライベートである。そのため、CSO は、テストのためにネットワークに接続する、DoD のテスト用暫定許可（IATT: Interim Authority to Test）、条件付き ATO、または PA と通常の DoD ポリシーに基づいて、構築前に、条件の有無にかかわらず DoD ATO を得なければならない。オフプレミスの商用インスタンス化のための以前の DoD PA は、オンプレミス IATT と ATO のアセスメントのみを告知する。以前の PA アセスメントの一部は、新たなインフラであることと場所が異なるので再評価が必要であるが、CSO インフラの場所が商用施設ではないので、C/CE 準拠の一部は DoD と特定の施設から継承される。仮想オンプレミスのシナリオにおけるインスタンス化は、レビューされたのと同じデータセンターでプライベートなインスタ化がホストされている場合、商用サービスおよびホストされている商用データセンターの DoD PA から、C/CE 準拠の一部を継承する。追加情報については、第 5.2.1.1 項「DoD オフプレミス Vs オンプレミス Vs 仮想オンプレミス」を参照。

上記のように、DFARS 条項 239.7602-1 (b) (2) (ii) は、CSP/CSO が契約授与に先立って DoD PA を有していなければならないという一般原則の例外を規定している。米国政府の施設から提供されるプライベートでオンプレミス CSO に対して契約が授与される可能性がある」と述べている。さらに、CSO は運用として使用する前に、PA を取得しなければならないと述べている。CSO を含むオンプレミスの DoD システムでは、運用として使用する前に ATO が必要である。この ATO は PA の代わりや、ミッションオーナーとその AO に利用される PA を生成するために使用される場合がある。

4.6 クラウドサービスとマネージド IT サービス

業界標準によれば、マネージド IT サービスは、顧客がテクノロジーと運用手順を指示するものであり、クラウドサービスの場合、プロバイダ（すなわち、CSP）がテクノロジーと運用

手順を指示するものである。契約者が元の CSP またはその他の組織であるかにかかわらず、契約者が運用する物理的または仮想オンプレミス DoD プライベート CSO は、通常の意味でのクラウドサービスではなくマネージドサービスである。これは、DoD が CSP の商用クラウドサービスの「コピー」または「バージョン」を DoD プレミス（仮想的または物理的）に構築し、プライベート CSO として運用/管理する契約を結んだ場合に発生する。マネージドサービスかクラウドサービスかは、サービス、インフラストラクチャ、および DoD が指定または指示するマネジメントの要件の数によって異なる。

DoD プライベートマネージドサービスは、商用クラウドサービスに対応した DoD ポリシーではなく、通常の DoD セキュリティ要件および RMF ポリシーに従う。マネージドクラウドサービスに適用されるセキュリティ要件には、この CC SRG の要件と標準の DoD RMF セキュリティ要件を含むとされている。

第5章 セキュリティに対する要求事項

CC SRG のこの章では、DoD のクラウドコンピューティング利用に関するセキュリティの必要条件を定める。以下のような様々な領域を包含している。

- ・ DoD の PA を得て DoD クラウドサービスカタログに掲載するための、CSO のアセスメントに対するセキュリティの要件
- ・ DoD のミッションをホストする CSP/CSO に対するセキュリティの要件
- ・ CSO 上のミッションオーナーのシステム／アプリケーションの利用や作成に対するセキュリティの要件

注意：この CC SRG の CSP と CSO への要求は、DoD へ提供または契約された全ての CSP と CSO に適用される。DoD は、CSO が DoD 契約の主要契約者として、CSP やインテグレータによって提供される可能性があることを認識している。DoD はまた、契約の条件を満たすためやシステムのメンテナンスのために、主契約者が複数の CSO を下請け契約者とすることを認識している。このため、この CC SRG の要件は、CSP の顧客情報へのアクセスや、CSO のセキュリティに影響を及ぼす可能性のある、主契約者から提供された CSO と、メンテナンスを含む下請け業者にも適用される。この下請けへのフロー・ダウンは、クラウドと契約関連の DFARS 条項にも含まれる。

5.1 セキュリティ管理策に対する DoD の方針

DoDI 8500.01 は、DoD の情報システムに対し、国家セキュリティシステム (NSS: National Security Systems) に該当するかどうかにかかわらず、CNSSI 1253 に沿った分類と、NIST SP800-53 として発行されているセキュリティ管理策および強化管理策 (C/CE) に従った実装を要求している。

CNSSI 1253 のベースラインは、FedRAMP のベースラインである NIST SP 800-53 の推奨ベースラインから展開したものである。

NSS やその他の情報については、NIST SP 800-59 「情報システムを国家セキュリティシステム」⁴³ として識別するためのガイドラインを参照。

5.1.1 DoD における FedRAMP セキュリティ管理策の利用

FedRAMP 低、中、高ベースラインは、NIST SP 800-53 セキュリティ管理策カタログで推奨されている低、中、高ベースラインを展開したものである。

2014 年 12 月 15 日の DoD CIO メモ、「調達と商用のクラウド・コンピューティング・サービス」では、「FedRAMP は、DoD サービスの最低限のセキュリティベースラインとしての役割

⁴³ NIST SP 800-59: <http://csrc.nist.gov/publications/PubsSPs.html>

を果たす」と述べている。この SRG では、すべての影響レベルについて FedRAMP の中ベースラインと、場合に応じて高ベースラインを考慮している。

レベル 2 : 2014 年の DoD CIO メモでさらに「公開されている格付されていない DoD の情報については、FedRAMP で認定されたクラウドサービスを利用してもよい」と述べている。セクション 3.2 の定義によれば、影響レベル 2 の情報は、セクション 5.6.2 「CSP の要員に対するセキュリティ要件」で概説されている要件と、ミッションオーナーと責任のある AO の受入れを条件として、少なくとも FedRAMP の中 (Moderate) PA と DoD レベル 2 の PA を保有した CSP でホストできる。FedRAMP の中ベースライン管理策は、影響レベル 2 の DoD PA として評価される。これは、DoD IT ミッションまたはミッションオーナーがレベル 2 CSO のシステム/Web サイト/アプリケーションのセキュリティを確保してホストしている中で、CSP がミッションオーナーから要求される CSP/CSO の他のセキュリティや構築の要件を満たすことを緩和するものではない。

レベル 4 : FedRAMP の中ベースライン、DoD が追加した FedRAMP+ C/CE やこの SRG におけるその他の要件が、影響レベル 4 の DoD PA の取得に向けた CSP の評価に利用される。

FedRAMP の高ベースラインと DoD レベル 4 FedRAMP+ C/CE の調整のため、DoD レベル 4 の PA 取得には別の方法がある。FedRAMP の高 PA については、追加の C/CE 評価なしで DoD レベル 4 PA として受理されるが、C/CE ベースの要求に該当しないアセスメントがこの SRG で要求される。

レベル 5 / 6 : DoD FedRAMP+ C/CE で強化された FedRAMP の中または高ベースラインとこの SRG の要求が、情報影響レベル 5 と 6 の DoD PA 取得に向けた CSP の評価に利用される。

FedRAMP PA のベースとして、どの C/CE ベースラインが利用されるせよ、レベル 4 / 5 / 6 の DoD PA の取得に先立って、アセスメントや認定には追加の考慮事項や要件が必要とされる。これらの考慮事項や要件は、この SRG を通して示されているが、セクション 5.1.7 「L4/5 DoD PA 取得のための追加の考慮事項と要件」の中で要約されている。

5.1.2 DoD の FedRAMP+セキュリティ管理策/強化

DoD FedRAMP+はセキュリティ C/CE のあつらえられたベースラインを指し、レベル 2 を除き DoD の各々の情報影響レベルについて開発されている。これらのベースラインには、FedRAMP 中または高ベースラインが組み込まれているが、これに限定されない。FedRAMP+ C/CE には、NIST 800-53 のセキュリティ管理策と、FedRAMP 中ベースラインに含まれていない強化機能が含まれている。FedRAMP+には、定義を必要とするほとんどの FedRAMP と FedRAMP+ C/CE のためのカスタマイズされた値と選択肢も含まれている。FedRAMP+ C/CE が選択された主な理由は、アドバンスド・パーシステント脅威 (APT:Advanced Persistent

Threat) やインサイダー脅威などの問題に取り組んでいることや、DoD は他の連邦政府とは異なって、CNSSI 1253 に従ってシステムを分類する必要がある、そのベースラインを使い、必要に応じて修正するためである。

DoD PA のサポートに使用される CNSSI 1253 ベースラインは、中程度の機密性と中程度の完全性に基づいている。可用性のベースラインは含まれていない (分類は M-M-x と標記されている)。可用性は FedRAMP のベースラインで扱われ、契約/ SLA のミッションオーナーによって対処される場合もある。その結果、得られた M-M-x ベースラインを FedRAMP 中ベースラインと比較して、各レベルの FedRAMP+セキュリティ管理策/強化のカスタマイズされたセットを導き出した。この比較から、FedRAMP 中程度ベースラインには、CNSSI 1253 M-M-x ベースラインにも含まれるが、NIST 800-53 中程度ベースラインには含まれていない C/CE が約 32 項目含まれていることが示された。この比較はまた、CNSSI 1253 M-M-x ベースラインの C/CE のうち 88 項目が、FedRAMP 中程度のベースラインにないことを示した。これらの 88 項目は、CSP 環境でのセキュリティ上の利点と CSP が C/CE を実装する必要がある場合の予測コストについて分析された。CSP を評価するための DoD クラウドベースラインの約半分が選択された。選択された管理策強化の数は、影響レベルによって異なる。

最近では、FedRAMP 高ベースラインの策定に伴い、DoD レベル 4 の FedRAMP+ C/CE の一部が値の調整を経て FedRAMP 高ベースラインに組み込まれた。

表 2 に、各情報影響レベルに適用される FedRAMP+ C/CE のリストを示す。追加の基本管理策は 3 項目だけである。残りは管理策の強化である。この表には、格付けされた情報またはプライバシーのオーバーレイによって追加された管理策は含まれていない。これらのオーバーレイにおける C/CE の評価に関する詳細は、この後のセクションで説明される。

注：この表には FedRAMP 中または高ベースライン C/CE は含まれていない。その表は FedRAMP Web サイト⁴⁴のドキュメントのページから入手できる。

⁴⁴ FedRAMP website: www.fedramp.gov/resources/documents

表 2 DoD FedRAMP+ セキュリティ管理策/強化

SP800-53r4 管 理策/強化 ID	FedRAMP+ for FedRAMP 中ベースライン			FedRAMP+ for FedRAMP 高ベースライン		
	レベル 4	レベル 5	レベル 6	レベ ル 4	レベ ル 5	レベ ル 6
AC-06 (07)	X	X	X			
AC-06 (08)	X	X	X			
AC-17 (06)	X	X	X			
AC-18 (03)	X	X	X			
AC-23	X	X	X			
AT-03 (02)	X	X	X			
AT-03 (04)	X	X	X			
AU-04 (01)	X	X	X			
AU-06 (04)	X	X	X			
AU-06 (10)	X	X	X			
AU-12 (01)	X	X	X			
CA-03 (01)		X	n/a*		X	n/a*
CM-03 (04)	X	X	X			
CM-03 (06)	X	X	X			
CM-04 (01)	X	X	X			
CM-05 (06)	X	X	X			
IA-02 (09)	X	X	X			
IA-05 (13)	X	X	X			
IR-04 (03)	X	X	X			
IR-04 (04)	X	X	X			
IR-04 (06)	X	X	X			
IR-04 (07)	X	X	X			
IR-04 (08)	X	X	X			
IR-05 (01)	X	X	X			
IR-06 (02)	X	X	X			
MA-04 (03)	X	X	X			
MA-04 (06)	X	X	X			

PE-03 (01)	X	X	X			
PL-08 (01)		X	X		X	X
PS-04 (01)		X	X		X	X
PS-06 (03)		X	X		X	X
SA-04 (07)		X	X		X	X
SA-12	X	X	X			
SA-19	X	X	X			
SC-07 (10)	X	X	X			
SC-07 (11)		X	X		X	X
SC-07 (14)			X			X
SC-08 (02)		X	X		X	X
SC-23 (01)	X	X	X			
SC-23 (03)	X	X	X			
SC-23 (05)		X	X		X	X
SI-02 (06)	X	X	X			
SI-03 (10)		X	X		X	X
SI-04 (12)	X	X	X			
SI-04 (19)	X	X	X			
SI-04 (20)	X	X	X			
SI-04 (22)	X	X	X		X	X
SI-10 (03)	X	X	X			
Total	5.1.5 参照	5.1.4, 5.1.5 参 照	5.1.4, 5.1.4.1 参照			
*レベル 5 FedRAMP+ C/CE の大半はレベル 6 にも適用可能。CA-03 (01) のレベル 6 での n/a の使用は、CE が「非格付け国家セキュリティシステム接続」に対するものであり、格付けされた NSS に対して選択または適用できないためである。						

注：CSP はケースバイケースで考慮される同等の管理策または低減を提案するかもしれない。

5.1.3 セキュリティ管理策と強化のパラメータ値

FedRAMP と DoD の双方は、セキュリティ管理策と強化パラメータの最小要件を定めている。しかし、状況によっては、実装の詳細が CSP に委ねられ、その実装が CSO と政府に適切かどうかについて評価される。FedRAMP と DoD が要求する管理策のパラメータ値は「付録 D-

PA の CSP 評価パラメータ値」で定義されている。追加のパラメータガイダンスについては、セクション 5.1.5.2 「CSP とミッションオーナーにおけるプライバシー・オーバーレイの影響」を参照。

5.1.4 国家セキュリティシステム (NSS)

すべてのレベルの管理策ベースラインは CNSSI 1253 のベースラインに基づいているが、影響レベル 5 と 6 は M-M-x まで分類された NSS (National Security Systems) に対応するように設計されている。これらのレベルには NSS 特有の C/CE が含まれており、これらのシステムには中程度のレベルよりもわずかに高い影響レベルが必要なもの（完全な高ベースラインには至らない）が含まれている。したがって、CSO が利用されている場合は、非格付けの NSS をレベル 5 でインスタンス化する必要がある。しかし、ミッション／情報の所有者が追加のセキュリティを要求する場合、これは、非格付けの非 NSS がレベル 5 で動作することを排除するものではない。

5.1.4.1 NSS レベル 6 格付けオーバーレイの適用性

影響レベル 6 は、定義上 NSS 用の格付けシステム用である。DoD RMF によれば、オンプレミス CSO は、FedRAMP および FedRAMP+に加えて、CNSSI 1253 格付け情報オーバーレイ⁴⁵の対象となる。このオーバーレイは、CNSSI 1253 の付録 F、CNSSI 1253F、別紙 5 「格付けされた情報オーバーレイ」に添付されている。これは CNSS ライブラリの指示されたページから入手できる。

このオーバーレイは、94 の追加の C/CE を課し、CSP の CSO レベル 6 の PA について評価されなければならない。すべての CSO には、CSP に適用可能な C/CE の一部のみが存在し、C/CE のバランスはミッションオーナーによって満たされる。この責任分担は、この文書の将来のリリースまたは付随文書で取り上げられる予定である。

5.1.5 CNSSI 1253 プライバシー・オーバーレイ

CNSSI 1253 プライバシー・オーバーレイは、CNSSI 1253F、付録 6、プライバシー・オーバーレイ⁴⁶と題された CNSSI 1253 の付録 F に添付されている。CNSS ライブラリの指示ページから入手できる。

プライバシー・オーバーレイは、1974 年のプライバシー法⁴⁷や HIPAA⁴⁸のような政府機関に適用される法律、政策、基準に見られる連邦のプライバシー要件に従い、両分野の専門家と弁護士を活用して開発された。C/CE を選択するか除外するか、補足ガイダンスと管理策

⁴⁵ Classified Information Overlay: <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>

⁴⁶ Privacy Overlay: <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>

⁴⁷ Privacy Act: <http://www.archives.gov/about/laws/privacy-act-1974.html>

⁴⁸ HIPAA: <http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html>

の拡張機能を提供するかどうかを含め、プライバシー・オーバーレイのすべての管理策仕様の基礎として法的参照が含まれている。これは、DoD や IC、ならびに CNSS の一部である他の連邦政府機関によってサポートされている。プライバシー・オーバーレイは、NSS の PII と PHI を保護するために CNSS によって作成されたが、システムが NSS であるかどうかにかかわらず、オーバーレイ仕様が基づいている多くの要件が PII または PHI を含む連邦情報システムに適用される。DoD を含むすべての連邦政府機関は、連邦政府の PII の収集、使用、および保守に適用される公法を遵守しなければならない。我々の知る限り、最良の情報源であることから、DoD は CNSS プライバシー・オーバーレイを呼び出している。

このオーバーレイは、低、中および高気密性の PII と PHI に言及している。それは、NIST SP 800-53 rev4、付録 J、プライバシー管理策カタログから 36 項目のプライバシー特有の C/CE の大部分を呼び出し、セキュリティ管理策カタログから追加の C/CE を呼び出す。また、FedRAMP 中および FedRAMP+ ベースラインですでに選択されている C/CE の多くを、パラメータ値の変更および管理策拡張とともに補足的なガイダンスを提供することによって変更する。追加の C/CE およびガイダンスの量は、PII 機密レベルと、PII が PHI の定義を満たすかどうかの両方に依存する。

5.1.5.1 レベル 2 における PII/PHI

PII と PHI は CUI に分類されているため、レベル 4 の CS0 に保存して処理する必要がある。プライバシー・オーバーレイは、低い機密性の PII のサブセットをオーバーレイの保護から除外する Business Rolodex Exception (BRE) を提供するが、これは CUI カテゴリからこの PII を削除するものではない。したがって、現時点では、PII/PHI はレベル 2 の CS0 で処理または保存することはできない。

5.1.5.2 CSP とミッションオーナーにおけるプライバシー・オーバーレイの影響

CC SRG の本体部分の分量に対するプライバシー・オーバーレイ C/CE とパラメータ値のリスト表示への影響を限定するために、このセクションでは、次のカテゴリでプライバシー・オーバーレイ C/CE の付録 E の表へのポイントを示す。

- ・ FedRAMP 中程度および FedRAMP+ C/CE は、管理策の拡張を通じて変更されるか、実装ガイダンスまたはバリュー仕様によって変更される。これらの表には、法律または規制によって要求される C/CE も含まれる。

- ・ 表 10-修正または規則から要求される FedRAMP M C/CE
- ・ 表 11-修正または規則から要求される FedRAMP+ C/CE

- ・ C/CE は、FedRAMP 中と FedRAMP+ C/CE を含む DoD クラウドベースラインには含まれていない。これには、SLA C/CE と呼ばれるいくつかの C/CE が含まれ、セクション 5.1.6 「契約／SLA のオプションで言及されるセキュリティ管理策／強化」が、FedRAMP+

や SLA C/CE セットに選択されなかった一部の CNSSI 1253 C/CE オプションとして扱われる。

- ・ 表 12 - FedRAMP M または FedRAMP + に含まれないプライバシー・オーバーレイ C/CE

- ・ 表 8 に定義されているパラメータ値を変更する可能性のあるオーバーレイによって定義されたパラメータ値を持つ FedRAMP 中および FedRAMP+ C/CE ベースラインにある C/CE - PA 評価のための FedRAMP M/FedRAMP+ 管理策/強化パラメータ値：

- ・ 表 13 - FedRAMP および FedRAMP + C/CE の PII / PHI パラメータ値

- ・ C / CE は、DoD クラウドベースラインには含まれない。これには、オーバーレイによって定義されたパラメータ値を持つ FedRAMP 中および FedRAMP+ C/CE が含まれる。

- ・ 表 14 - FedRAMP M または FedRAMP+ に含まれていない C/CE の PII/PHI パラメータ値

注：プライバシー・オーバーレイ C/CE のさまざまな他のベースラインに対する比較分析は、付録 F で提供されている。この比較は、さまざまなカテゴリの C/CE の統計またはカウントを提供している。これは情報提供のみを目的として提供されており、CC SRG の最終版または将来のリリースから削除される可能性がある。

5.1.5.3 プライバシー・オーバーレイ管理策/強化の CSO アセスメント

PII や PHI（特定の SaaS および PaaS 提供など）を保存・処理しようとする CSP CSO は、CSO の DoD PA を得るために、FedRAMP+ C/CE と FedRAMP の中ベースラインに対するプライバシー・オーバーレイの追加・修正に対し、評価を追加する必要がある。これには、適切なレベルで FedRAMP+ テーブルに追加されるオーバーレイに+シンボルを示す CNSSI 1253 M-M-x ベースライン（FedRAMP + C / CE の選択に使用）からのすべての SLA C/CE および選択されていない C/CE が含まれる。

プライバシー・オーバーレイのアセスメントに合格した場合、PII または PHI のレベルを参照して、CSO が首尾よく評価された PII または PHI のレベルを参照する DoD の PA を得ることができる。例えば、CSO xyz に、レベル 4 の PA が付与され、中程度の機密性の PII までの処理、または PII と PHI のあるレベルを処理するための追加の暫定認可が付与される。プライバシー・オーバーレイ C/CE は、CPS の顧客である DoD ミッション/情報の保有者（すなわち、TR-2 につき、SORN (Systems of Record Notice) が必要）の明確な責任であり、DoD の PA の取得には影響しない。

また、IaaS および一部の PaaS CSO は PII や PHI を保存・処理する可能性があるが、これは主に利用者の裁量に委ねられており、通常は CSP の意向ではない。このように、IaaS と

一部の PaaS CSO が DoD PA を受け取るためにプライバシー・オーバーレイ評価は必要とされない。

さらに、CSP の IaaS および一部の PaaS CSO は通常、プライバシー・オーバーレイに対して評価されないが、ミッションオーナーが CSO で PII や PHI の保管と処理を選択した場合、CSP の責任となる C/CE が存在することが認識されている。通常、これらの C/CE の評価は、ミッションオーナーによって CSP と交渉される。

注：一部の PaaS CSO は、一部の SaaS CSO のように PII/PHI の処理を行う。これらは通常、SaaS CSO に非常によく似ており、プライバシー・オーバーレイに対して評価する必要がある。

DISA は、DoD PA におけるプライバシー規定を含め、CSO のプライバシーのアセスメントを実施していない。ミッションオーナーが、使用された P/SaaS CSO のプライバシー・オーバーレイアセスメント、および I/PaaS 上に構築されたアプリケーションの責任を負う。プライバシー・オーバーレイ C/CE が CSP とミッションオーナーのどちらに適用されるかに関する具体的なガイダンスは、この SRG の将来のリリースで提供される予定である。

5.1.5.4 プライバシー・オーバーレイ管理策／強化のミッションシステム／アプリケーションアセスメント

ミッションオーナーのクラウドシステム／アプリケーションが PII や PHI の保存や処理を目的としている場合、システム／アプリケーションは、プライバシー・オーバーレイに記載されているプライバシー要件を既に満たしている必要がある。したがって、PA の乗り手を含むプライバシー・オーバーレイ評価は、ミッションオーナーの CSP 評価／選択／取得プロセスと、ミッションシステムの ATO に対する評価プロセスに組み込む必要がある。

注：プライバシー・オーバーレイ C/CE が CSP とミッションオーナーのどちらに適用されるかに関するより具体的なガイダンスは、この SRG の将来のリリースで提供される予定である。

5.1.6 契約／SLA のオプションで言及されるセキュリティ管理策／強化

表 3 は、デフォルトで含まなければならない FedRAMP および FedRAMP+ C/CE を超えて、ミッションオーナーが契約または SLA でオプションとして対処するように指定された C/CE を示している。これらの C/CE は、一般的にシステムの可用性に関するものであるが、継続的な監視、インシデントレスポンス、およびその他のセキュリティの問題に関する情報の可

用性に適用される。これらの C/CE への遵守に関するアセスメントと継続監視は、ミッションオーナーの責任である。

このリストは、システムやアプリケーションを安全にするために CSP によって提供される管理策／強化が必要とされるならば、契約／SLA における CNSSI 1253 ベースラインまたは NIST SP 800-53 rev4 からミッションオーナーが管理策または強化に言及することを排除するものではないことに注意する必要がある。これらの C/CE への遵守の評価と継続的な監視は、ミッションの ATO の達成と維持において CSP と調整したミッションオーナーの責任である。これらの C/CE は、現時点では、DoD PA の授与に向けて評価されていない。

表 3 契約/SLA で対処されるセキュリティ管理策/機能強化

SP 800-53r4 管理策／強化 ID	レベル 4	レベル 5	レベル 6
AC-02 (13)	X	X	X
AC-03 (04)	X	X	X
AC-12 (01)		X	X
AC-16	X	X	X
AC-16 (06)	X	X	X
AU-10		X	X
IA-03 (01)	X	X	X
PS-04 (01)	X		
PS-06 (03)	X		
SC-07 (11)	X		
SC-07 (14)	X		
SC-18 (03)			X
SC-18 (04)		X	X
Total	9	10	9

5.1.7 L4/5 DoD PA 授与のための追加の考慮事項と要件

以下は、レベル 4／5／6 PA が授与される前に、AO 受け入れのためのセキュリティ管理策アセスメントに加えて、またはそれと併せて評価またはレビューされなければならない考慮事項と要件のリストである。このリストはすべてを網羅しているわけではなく、具体的な要件は、現時点で十分に開発されていない可能性がある。

DoD が評価する検討事項や要件には、以下が含まれるが、これに限定されるものではない。

- DoD 特権ユーザおよび非特権ユーザによる DoD PKI 認証のサポートはどのように実装されているか。これには、それらの実装と共に使用されるプロセスとプロトコルを含む。たとえば、SAML アサーションが使用されている場合、関与しているサーバー、アサーションフロー／ステップ、およびユースケースの保護方法。

注：現時点では、CC SRG に SAML ガイダンスは提供されていない。

- 関連する CC SRG セクション：
 - ・ 5.4、CSP の DoD 公開鍵インフラストラクチャ (PKI) およびサブセクションの使用。
 - ・ 5.10.7、クラウドとサブセクションの Active Directory 統合
- DoD IP アドレッシングのサポートがどのように実装されているか
 - 関連する CC SRG セクション：
 - ・ 5.10.4.1、IP アドレッシング。この考え方は、商用 IP アドレスを NIPRNet 経由でルーティングする必要性に対処している。
- CSP PA が授与される CSO をホストするデータセンターのロケーション。
 - 関連する CC SRG セクション：
 - ・ 5.2.1、管轄／所在地要件
- CSO 管理／監視プレーン（または特定のデバイス／システム）、および CSP の企業ネットワークまたは一般商用 CSO 管理プレーンとの統合

注：現時点ではこの対価に関する詳細は記載されていないが、関連する懸念事項については次の項目を参照

- 関連する CC SRG セクション：
 - ・ 5.10.2.3、管理プレーンの接続性
- CSO インフラストラクチャを管理・監視する CSP 要員。これは主に、前の項目に関する米国人の制約に関連している。
 - 関連する CC SRG セクション：
 - ・ 5.6.2、CSP 要員の要件。
- BCAP および meet-me ポイントによる接続をサポートするために、構外の CSP/CSO のネットワークと DoD ネットワーク間のプライベート接続機能が利用可能であること。
 - 関連する CC SRG セクション：

- 5.10.1、クラウドアクセスポイント（CAP）およびサブセクション
 - 5.10.1.1.2、NIPRNet BCAP Meet-Me ポイント
 - 5.10.1.1.3、BCAP 接続のための CSP サポート
- パブリック DNS やコンテンツ配信ネットワークなどのインターネットベースの機能に対する CSO やユーザエクスペリエンスの依存。そのようなすべての機能は、CSO インフラストラクチャと DISN BCAP 経由での接続を介して利用可能でなければならない。紛争の時または DISN/DoDIN が攻撃されて、DoD がインターネットへのアクセスを制限したりインターネットから切断したりする場合でも、CSO は機能する必要がある。

注：ここに記載されている以外の特定の要件はない。

- 関連する CC SRG セクション：
 - 5.10.4.2、ドメインネームサービス（DNS）。
- NIPRNet または CSO のいずれかから、CSO 管理／サービス要求ポータルまたは API エンドポイントにアクセスするためのインターネットアクセスへの依存。すべてのそのようなアクセスは、NIPRNet からの場合は CAP 経由でなければならない、CSO 内からの場合は CSP/CSO のネットワーク上にとどまる必要がある。これらの要件は、永続的なものではない場合は、最小限で構成可能でなければならない。

注：ここに記載されている以外の特定の要件はない。

- 関連する CC SRG セクション：
 - 5.10.1、クラウドアクセスポイント（CAP）およびサブセクション
- CSP のネットワークと CSO の保護機能により、CSP/CSO のネットワークと CSO へのインターネット接続が BCAP を介したプライベート接続を介して NIPRNet のバックドアになることを防止する。
 - 関連する CC SRG セクション：
 - 5.10.1.1.4、インターネットと BCAP への CSP / CSO ネットワーク接続性。
- インターネットベースの脅威からの保護のために、インターネットと CSO の間に実装された CSP の必要な境界保護（多層防護によるセキュリティ/防御対策）の堅牢性。この保護は、CSO が I/PaaS か、または P/SaaS であるか、およびミッションオーナーが CSO の一部を支配するかどうかによって異なると予想される。
 - 関連する CC SRG セクション：
 - 5.10.3、CSP サービスアーキテクチャとサブセクション
- この SRG の残りの部分で定義されているその他すべての要件

- CSO を評価している間、または教訓の結果として実現されたその他の考慮事項。

5.2 法的留意事項

このセクションでは、DoD の情報の所在を中心とした法的要件と、CSP 施設と CSO の誰がアクセスできるのかについて説明する。

5.2.1 管轄/所在地要件

DoD と米国政府のデータがどこにあるかについての情報管理に関する法的管轄権。これは、DoD プレミスにおける情報によって微妙に異なる。

米国以外の者や政府機関による差押えや不適切な使用から保護するために、DoD によって保管され、処理されるすべてのデータは、米国の排他的な法的管轄下の施設に所在していなければならない。CSP は、DoDI 8510.01 に記述されているように、責任ある AO の別段の承認がない限り、50 州、コロンビア特別区、および米国の外圏（FAR 2.101⁴⁹で定義されている）内の DoD 施設に物理的に配置されていないすべての政府データを維持する。

請負の責任者は、請負業者が 50 州以外の場所、コロンビア特別区、および米国の外来地域で政府のデータを維持することが許可されている場合、請負業者へ書面で通知するものとする。

CSP は、いつでもデータが保存される物理的な場所のリストを機関へ提供し、新しい物理的な場所が追加された場合はリストを更新するものとする。

オンプレミス CSP や CSO を使用してオンプレミス CSO を拡張するか、または実質的に DoD フェンスライン（DISN 境界）を拡張するハイブリッドモデルを使用する DoD または非 DoD CSP によって実装されたオンプレミス CSO も、ここで述べた所在地の要件を満たさなければならない。

対応するセキュリティ管理：SA-9（5）

5.2.1.1 DoD オフプレミス 対 オンプレミス 対 仮想オンプレミス

DoD オンプレミス対オフプレミスは、施設または IT インフラストラクチャの物理的または仮想的な場所に関係している。

DoD オフプレミス：施設（建物／コンテナ）または IT インフラストラクチャが、物理的にまたは事実上 DoD が所有または管理する敷地（すなわち、オンプレミス）でない場合は、

⁴⁹ FAR 2.101:

<http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/02.htm>

オフプレミスである。以下の DoD オンプレミスと DoD 仮想オンプレミスおよび詳細については付録 B の定義を参照。

DoD オンプレミス：施設（建物／コンテナ）または IT インフラストラクチャが、物理的に DoD の所有または管理された敷地であれば、オンプレミスにあたる。つまり、DoD の要員による DoD セキュリティポリシーの直接管理下にある DoD の施設（ベース、キャンプ、ポスト、ステーション（B/C/P/ S）または賃貸商業スペース）の保護された境界線（壁または「フェンス線」）内である。

DoD オンプレミスには、DoD のデータセンター、DoD の B/C/P/S にあるその他の施設、または商業施設またはその他の政府施設（またはその一部）が含まれる。この意味での商業施設とは、DoD によってリースされ管理されている建物またはスペースを意味する。このような施設は DoD が管理する施設または施設の保護された境界線または「フェンス線」内にあるとみなされる。物理的設備は、恒久的な建物または輸送／輸送コンテナなどのポータブル構造であってもよい。後者の例として、コアデータセンター（CDC: Core Data Center）に隣接し、建物内にあるかのようにネットワークに接続された商用 CSP のインフラストラクチャを収容する輸送コンテナが該当する。

DoD の CSP は、商用 CSP が（DoD の契約下で）DoD 構内（DoD オンプレミス）で CS0 アーキテクチャをインスタンス化することができる。DoD ネットワークとの相互接続は、サイバーセキュリティのガイダンスと管理策を満たす技術要件に基づいて相互運用が可能である。そのような実装は DoD プライベートとみなされる。

DoD 仮想オンプレミス：連邦政府や商用データセンターなどの物理的に建物外の場所（施設）にある DoD プライベート IT や CS0 インフラストラクチャ（すなわち、DoD 以外のセキュリティポリシーで DoD 以外の人員が直接管理する施設）は、以下に列挙された特定の条件の下で、事実上のオンプレミスとみなすことができる。これらの条件は、特定の物理的セキュリティ管理策を適用し、DISN 認定の境界の拡張である。本質的には、このような構築は、インフラストラクチャの周りに DoD の保護された境界または「フェンスライン」の仮想的な拡張である。また、IT/CS0 インフラストラクチャと管理プレーンを 1 つまたは複数の DISN エンクレープに配置することで、専用の DoD ICAP/BCAP の代わりにインフラストラクチャを提供する CS0 を使用するなどの境界保護の代替アプローチを実現している。

IT/CS0 インフラストラクチャは、以下の条件の下で、仮想オンプレミスとみなすことができる。

- CS0 インフラストラクチャが DoD プライベート／コミュニティであり、そのインフラ

ストラクチャ、デバイス、モニター／サポートインフラストラクチャ、管理プレーンは専用であり、データセンター内の他のインフラストラクチャ、デバイス、ネットワークエンクレーブから物理的に分離されている。

- DISN トランスポートが、CSO インフラストラクチャ、CSO 監視／サポートインフラストラクチャ、および CSO 管理プレーンをサポートする CSO のネットワークエンクレーブに拡張されている。
- エンクレーブ／データセンター境界保護が、DISN エンクレーブ境界またはコアデータセンタ（CDC）の保護要件を満たす CSO 運用エンクレーブ（CSO 監視／サポートインフラストラクチャを含む）を保護するために実装されている。
- CSO インフラストラクチャが、CSO の管理専用の 1 つまたは複数のエンクレーブから管理される。これは、エンクレーブ内の専用のワークステーションを使用するか、またはリモートからの専用の仮想デスクトップインフラストラクチャ（VDI）の利用である。
- エンクレーブ境界保護が、DISN エンクレーブの境界保護要件を満たすために、専用の CSO 管理／監視／サポートエンクレーブを保護するために実装されている。
- CSO インフラストラクチャが、DISN ネットワークデバイスや CSO インフラストラクチャを収容するために使用される商用データセンター内のケージや部屋（または、少なくとも、DoD スペースを閉鎖する取外し不可能な側面を有する 1 つまたは複数のロックされたキャビネット）などの物理的に分離／保護されたスペースに収容されている。関連 C/CE：PE-3、PE-3（1）*、PE-3（4）*、PE-4
- この物理的に離れたスペースが、少なくとも以下のように保護される。
 - データセンターへの物理的アクセスが、FedRAMP の中または高ベースラインにおけるすべての必要な物理的および保守要員のアクセスセキュリティ管理策に準拠し、要員の役割ベースのアクセス制御、アクセス監査、訪問者のアクセス制御、必要に応じたエスコートを含むが、これに限定されない。関連 C/CE：MA-5、MA-5(1)、PE-2、PE-2（3）*、PE-3、PE-3(1)*、PE-6、PE-6(1)、PE-6(4)*、PE-8
 - DoD スペースへの物理的アクセスが、FedRAMP の中ベースラインまたは必要に応じて高ベースライン（データセンターについて上で説明したとおり）または適切な CNSSI 1253 ベースラインにおける必要なすべての物理的および保守要員のアクセスセキュリティ管理策に準拠している。

注：機密システムを収容する施設には、追加または代替の物理的セキュリティおよび人員管理が必要な場合がある。

- 要員のアクセスが、トークンやバイオメトリックベースの自動入室アクセス制御システム（AECS: automated Entry Access Control System）によって制御される。このシステムは、DoD の管理下もしくは施設所有者の管理下にあり、許可された個

人だけにアクセスを制限し、アクセスおよび退出する人物のアイデンティティを含むすべてのアクセスを記録／監査し、無許可のアクセスや失敗した試行についてはアラートとログを提供しなければならない。関連 C/CE : PE-6、PE-6 (1) および PE-6 (4) *

- 。 物理スペースへのアクセスが、ビデオカメラおよび物理的侵入検知システム (PIDS: Physical Intrusion Detection System) (すなわち、侵入警報システム) を使用して施設の所有者によって外部から監視される。関連 C/CE: PE-6、PE-6 (1)、PE-6 (3) *、および PE-6 (4) *
- 。 DoD が運用する自動モーションアクティベーション PIDS やビデオカメラで、内部空間を監視することが強く推奨される。このようにして、DoD は、空間内の許可されたまたは許可されていないすべての要員の活動を監視することができる。関連 C/CE : PE-6、PE-6 (1)、PE-6 (2) *、PE-6 (3) *、および PE-6 (4) *

5.2.2 クラウド展開モデルの考慮事項／分離要件

様々なタイプの DoD の情報が処理または記憶されるなかで、仮想化技術を使用する際のリスクと法的な考慮事項により、同じ物理インフラストラクチャ上の仮想化環境からクラウドサービスを取得できるテナントの種類や、クラウド展開モデルの種類（公開、プライベート、コミュニティ、ハイブリッドなど）がさらに制限される。

共有されたクラウド環境は DoD エンティティにとって重要な機会を提供するが、対処すべき DoD データやシステムにも固有のリスク生じる。これらのリスクには、仮想化技術における脆弱性の悪用、外部システムへのインターフェース、API や管理システムが含まれる。これらは、利用者のシステムおよびデータへのバックドア接続や CSP 特権ユーザアクセスを提供する可能性がある。仮想環境と物理環境を適切に構成することで、これらの脅威の多くを軽減することができるが、DoD が許容可能または許容できない残存リスクが存在する可能性がある。非政府な CSP 顧客／テナントのデータの e ディスカバリや法執行などの法的懸念は、DoD データが同じストレージメディアにある場合、DoD データに脅威を与える。これらの懸念から、DoD は現在レベル 5 の情報に関して慎重なアプローチをとっている。

インフラストラクチャ（クラウドサービスに関連するもの）は、物理的なハードウェア（サーバーおよびストレージ）やクラウドサービスをサポートするハードウェアと、その仮想化技術（使用されている場合）を相互接続するネットワークである。これには、インフラストラクチャを管理するために CSP によって使用されるシステムとネットワークが含まれる。このインフラストラクチャが収容されている物理空間は CSP のインフラストラクチャの一部であるが、これはレベル 6 以外における DoD の分離制限の要因ではない。

専用インフラストラクチャ（クラウドサービスに関連するもの）とは、単一の顧客組織または特定の顧客グループにサービスを提供することに専念するクラウドサービスインフラストラクチャを指す。プライベートクラウドサービスは、1つの顧客組織にサービスを提供する専用のインフラストラクチャの実装である。このSRGは、DoDをすべてのDoDコンポーネントで構成される組織と見なしている。このSRGは、DoDのプライベートクラウドをDoD利用者とテナントにサービスを提供する専用のインフラストラクチャとして限定し、これをDoDプライベートクラウドと称している。DoDのプライベートクラウドまたはクラウドサービスの提供は、すべてまたは一部のDoDのコンポーネントにサービスを提供するマルチテナントである場合もあれば、単一の任務を担う単一のテナントである場合もある。コミュニティクラウドサービスは、特定のグループまたは顧客組織のクラスにサービスを提供する専用のインフラストラクチャを実装している。DoDプライベートの定義はDoDコミュニティクラウドと見なすこともできるので、このSRGはDoDプライベート／コミュニティという用語を使用している。このSRGでは、連邦政府のコミュニティという用語も使用される。これは、DoDコンポーネントとミッションオーナー、ならびに他の連邦政府機関とミッションオーナーの両方にサービスを提供する専用のマルチテナントインフラストラクチャを意味している。

対応するセキュリティ管理策：SC-4

5.2.2.1 影響レベル2 場所と分離の要件

影響レベル2のクラウドサービスは、4つの展開モデルのいずれかで提供できる。影響レベル2で処理および保存できる情報は、セクション5.2.1「管轄／所在地要件」で説明されているように、情報の物理的な場所が制限されている限り、オンプレミスまたはオフプレミスで処理可能である。レベル2のPAの場合、DoDは、これがFedRAMP中(moderate)のPAによって適切に対応されているというリスクを受け入れているため、レベル2のPAに関して要件が追加で評価されることはない。

5.2.2.2 影響レベル4 場所と分離の要件

影響レベル4のクラウドサービスは、4つの展開モデルのいずれかで提供できる。影響レベル4で処理および保存できる情報は、セクション5.2.1「管轄／所在地要件」で説明されているように、情報の物理的な場所が制限されている限り、オンプレミスまたはオンプレミスで処理できる。

レベル4のPAの場合、CSPは、強力な仮想分離管理策と、Doの情報とデータの開示なしでDoD以外の情報とデータに対する「検索と押収」要求を満たす能力を裏付ける証拠を提供しなければならない。さらに、強力な仮想分離管理策は、他のCSP顧客と同じ物理ハードウ

ウェアを使用している 1 人の CSP 顧客が他の情報／データ、仮想ネットワーク、または仮想マシンにアクセスできる潜在的な脆弱性を防止／緩和／除去する必要がある。監視は、そのような不正アクセスや侵入を検知し、インシデントレスポンスが可能となるようにする必要がある。

5.2.2.3 影響レベル 5 場所と分離の要件

影響レベル 5 で処理・保存の必要がある情報は、セクション 5.2.1「管轄／所在地要件」で説明されているように情報の物理的な場所を限定するクラウド展開モデルのオンプレミスまたはオフプレミスの DoD プライベート／コミュニティまたは連邦政府のコミュニティクラウドでのみ処理できる。

以下も適用される：

- DoD の民間／コミュニティまたは連邦政府のコミュニティクラウドのみが影響レベル 5 の対象となる。
- 各展開モデルは、各顧客組織から複数のミッションまたはテナント／ミッションをサポートすることがある。
- DoD と連邦政府のテナント／ミッション間の仮想的／論理的な分離で十分である。テナント／ミッションシステム間の仮想的／論理的な分離は最低限必要である。
- 非 DoD/非連邦政府のテナント（すなわち、公共、地方／州政府のテナント）からの物理的分離が必要である。
- CSP は、DoD およびコミュニティの情報への潜在的なアクセスを米国市民である CSP 従業員に制限する。

注：ITAR に準拠して販売されているマルチテナント CSO の場合、「政府クラウド」または「政府のためのクラウド」はデータの所在地を米国の管轄区域に制限し、CSO を管理する人員を制限する可能性があり、連邦政府または DoD の「専用」として利用している。クラウドサービスまたはその基盤となるインフラストラクチャが、連邦政府以外のテナント（州政府、地方政府、部族政府、業界／学術パートナー、または外国政府など）をホストしている場合は、この SRG の目的からパブリッククラウドとみなされる。したがって、DoD はこれをレベル 4 に適切と見なすが、ここで説明された属性は、レベル 5 ミッションの DoD ミッションオーナーによる CSP 選択には不十分である。この制限は、CSP と CSO がテナントの作業量とデータや一般的な政府のコミュニティと連邦政府のコミュニティとの間の十分な分離を証明できる場合、DoD によって免除される可能性がある。

5.2.2.4 影響レベル 6 場所と分離の要件

影響レベル 6 は、SECRET までに分類された情報の保管と処理のために予約されている。影響レベル 6 で処理・保存する必要がある情報は、セクション 5.2.1「管轄／所在地の要件」で説明されているように、情報の物理的な場所を限定したクラウド展開モデルのオンプレミスまたはオフプレミスの DoD プライベートコミュニティまたは連邦政府のコミュニティクラウドでのみ処理できる。

以下が適用される：

- SECRET レベルまでの影響レベル 6 情報は、保管や処理される情報の最高レベル以上の格付けの機密情報の処理のために認可された施設に位置する、専用のクラウドインフラストラクチャに格納され、処理されなければならない。
- 影響レベル 6 の CS0 インフラストラクチャは SIPRNet エンクレープとみなされ、SIPRNet にのみ接続された CS0 処理、ストレージ、および管理プレーンの独立した環境になる。
- 各導入モデルは、複数の顧客組織からの複数の SECRET ミッションをサポートすることができる。
- DoD と連邦政府のテナント／SECRET ミッションは、仮想的／論理的な分離で十分である。
- テナント／ミッションシステム間の仮想的／論理的な分離は最低限必要である。
- 非 DoD／非連邦政府のテナント（換言すれば、公共、地方／州政府のテナント）からの物理的分離が必要である。

5.2.2.5 法執行と刑事捜査と E ディスカバリの支援における分離

連邦政府の法律に基づき、連邦政府は、連邦政府の従業員と選出された当局者、並びに連邦政府への不正行為、そのようなデータの誤用、または事件の調査に関する情報を入手できる人物に対する犯罪捜査の権利を留保している。このような犯罪捜査には、デジタル証拠を収集するための連邦政府情報に関する E ディスカバリの必要性が含まれる場合がある。したがって、CSP は、連邦政府の情報を非連邦政府の情報から CS0 内で分離することができなければならない。分離の粒度は、連邦政府のミッションオーナーレベルでなければならない。CSP はまた、この分離要求がすべての CSP／インテグレータの下請けの CSP/CS0 まで流れる必要がある。CSP と下請け業者は、契約上の担当官の要請に応じて、または召喚状に応じて、1 つまたは複数の連邦政府ミッションオーナーのデータを、要求された連邦政府の情報のフォレンジック・デジタル・イメージの提供や CSP の関与なしに、契約担当官によって確認され、許可された政府の要員のみにアクセスを限定されたセキュアな遠隔接続か、またはセキュアな場所で、レビュー、スキャン、または法的に評価される環境に隔離することができなければならない。フォレンジック・デジタル・イメージのキャプチャと保護の詳細につ

いては、セクション 6.5.4「クラウドにおけるデジタルフォレンジックと法執行／犯罪捜査のサポート」を参照。

5.2.3 DoD データの所有権と CSP による DoD データの使用

DoD ユーザが CSP の CSO に配置または作成したすべての DoD の情報／データは、DoD との契約で別段の定めがない限り、DoD、ミッションオーナーやその情報の所有者の所有である。CSP には、DoD の情報／データに対する権利はない。DoD の情報／データには、IaaS/PaaS CSO に実装されたミッションオーナーのシステム／アプリケーション内で作成されたログと監視データ、および CSO の使用と管理に関するミッションオーナーに対して作成され提供されたログが含まれる。また、DoD は、DoD のための CSP/CSO によって作成されたすべての情報／データの所有権を、そのようなアクティビティが契約の一部である場合は保持する。DoD PA を取得する CSP は、DoD が CSO のすべての DoD データの所有者であることに同意する必要がある。

CSP は、DoD に契約サービスを提供するために必要な（例えば、請求のために使用される顧客アクセス／使用ログ）以外の DoD のデータを使用することを禁じられている。これは、契約書に規定されている以外の目的で、CSP が DoD の電子メール、ファイル、データベースの中の情報や通信をマイニングすることはできない。

CSP は、ミッションオーナーの CSO の使用および管理に関連して、CSO 内で作成されたすべてのログおよび監視データの所有権を保持している。これには、顧客のアクセスおよび課金に利用される使用に関するログ、CSO の容量計画に使用されるデータ、悪意のある活動または CSO の稼働状況に関するデータの監視が含まれる。これは、AU-11 で指定された期間、AU-2 セキュリティ管理策で指定されたすべての監査内容も含まれる。CSP はこの情報の所有権を保持しているが、プランニング、フォレンジック、請求の検証、保持などの目的で、ミッションオーナーと共有する必要がある。DoD／ミッションオーナーと共有するこの情報のコピーの所有権は、DoD／ミッションオーナーによって維持管理される。

さらに、ミッションオーナーと共有されるすべての DoD の情報／データおよび CSP の情報／データは、セクション 5.8「CSO から移行のためのデータ処理と破棄」、セクション 5.12「バックアップ」に従って、オフボードとバックアップを利用可能にする必要がある。

ミッションオーナーは、契約におけるデータ所有権を規定する必要がある。

関連セキュリティ管理策:AC-23

5.3 継続的な評価

FedRAMP と DoD の両者は、DoD へサービスを提供する CSO に対して継続的な評価と認可能力を要求している。この能力は、FedRAMP⁵⁰および FedRAMP 継続的モニタリング戦略ガイドの理解のためのガイド⁵¹に記載されているように、DoD RMF と FedRAMP の継続的モニタリング戦略に基づいている。これらの進行中の評価プロセスには、継続的な監視と変更管理が含まれる。

継続的アセスメントの評価プロセスは、影響レベルによって異なるわけではないが、そのプロセスの一部として生成される成果物が影響を受ける可能性がある（例えば、レベル 2 の CSO は、レベル 4 の CSO よりも監視するコントロールが少ない）。しかし、これらのプロセスは、CSO が FedRAMP カタログの一部であるか、または FedRAMP JAB PA であるかによって異なる。これらの違いは、一連のセキュリティ管理策に対する責任分担と、FedRAMP プロセスの一部として生成された成果物にアクセスする DoD の能力に基づいている。

継続的アセスメントの責任は、クラウドシステムに固有の責任と統制を分担している。FedRAMP のプロセスは、FedRAMP カタログのすべての CSO に対して活用される。ただし、このプロセスでは、FedRAMP 中のセキュリティ管理策など、FedRAMP PA が管理するシステムの部分のみが対象となる。DoD の変更管理プロセスは、DoD が管理するシステムの一部（FedRAMP+セキュリティ管理策など）に適用される。ミッションオーナーから要求されて SLA に規定されているような、FedRAMP または DoD PA に該当しない管理策の継続的な評価は、ミッションオーナーの責任である。このアセスメントの責任分担を図 3 に示す。

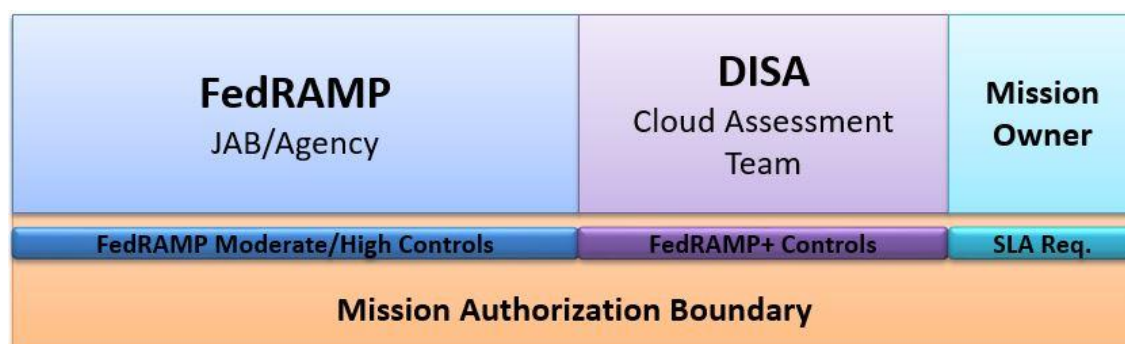


図 3 継続的アセスメントの責任分担

⁵⁰Guide to Understanding FedRAMP: <https://www.fedramp.gov/resources/documents/>

⁵¹ FedRAMP Continuous Monitoring Strategy Guide: <https://www.fedramp.gov/resources/documents/>

5.3.1 継続的モニタリング

このセクションは、CNSSI 4009 と NIST SP 800-137 で定義されているように、セキュリティ管理策の継続的な監視に特に関係している。コンピュータネットワーク防衛の一部として実施される監視活動に関する詳細は、第 6 章「サイバー空間防御とインシデントレスポンス」で説明されている。

DoD PA が付与されると、CSP は、継続的かつ定期的な脆弱性スキャン、DoD 年次アセスメント、インシデント管理、運用プロセスと手順の効果的な実施を通じて、CSO のセキュリティ態勢を維持することが期待される。これには、適切な AO への定期的な報告が不可欠である。DoD PA を維持するために必要な継続的な監視の成果物は、FedRAMP が要求するものと同じである（年次評価、月次脆弱性スキャンなど）。ただし、これらの成果物には、FedRAMP+ コントロールおよび DoD の要件に関する追加情報が含まれている必要がある。

継続的なモニタリングのデータフローは、CSP が FedRAMP JAB PA、非連邦機関の ATO によるアセスメントを受けた 3PAO、または DoD がアセスメントを行った PA（セクション 0 で説明）を持っているかどうかによって、CSP による違いがある。これらのデータフローは、それぞれ図 4、図 5、および図 6 に反映されている。

いくつかのケースでは、例えば DoD プライベート CSO や非 DoD の機関 ATO の FedRAMP カタログの中の CSO のような CSP が直接 DISA へモニタリングの成果物を提供する。そのような場合、CSP は、DoD が継続的な監視データの取り込みの自動化を可能にする商用標準フォーマット（例えば、コンマ区切り値、XML）を利用する。

注:XML 交換の場合、国家情報交換モデル(NIEM: National Information Exchange Model)ベースの XML が、DoDI8320.07⁵²（2015 年 8 月 3 日）に従った推奨のフォーマットである。このフォーマットに関する追加情報は、www.niem.gov を参照。

すべての CSP CSO は、FedRAMP PA の維持のために 3PAO によって FedRAMP の年次アセスメントを実施することが求められている。また、DoD は、3PAO または承認された DoD SCA 組織が、レベル 4 以上の DoD PA を維持するために実施する年次アセスメントを要求している。FedRAMP と DoD カタログの両方の CSO は、FedRAMP と DoD の両方に対するこの要件をカバーするために、1 回の年次アセスメントを受けることが期待されている。FedRAMP カタログの CSO は、FedRAMP 継続的モニタリング戦略ガイド(Continuous Monitoring Strategy Guide⁵³)

⁵² DoDI 8320.07: <http://www.dtic.mil/whs/directives/corres/pdf/832007p.pdf>

⁵³ FedRAMP Continuous Monitoring Strategy Guide: <https://www.fedramp.gov/resources/documents/>

に記載されているプロセスに従う。DoD の年次アセスメントには、少なくとも付録 A に列挙されている管理策のセットと、DISA AO によって指定されたその他の管理策を含む。FedRAMP カタログにない DoD PA の CSO は、継続的なモニタリングとそれに関連する評価のために DoD RMF プロセスに従う。

対応するセキュリティ管理策：CA-7

5.3.1.1 DoD PA と FedRAMP カタログの CSO の継続的監視

セクション 4.1 「商用／Non-DoD クラウドサービスのアセスメント」で説明したように、DoD の対象となる FedRAMP カタログの CSO には、JAB PA (3PAO で評価された) または 3PAO で評価された連邦政府機関 ATO を持つ CSO が含まれている。これらの CSO のための自己アセスメントを含む FedRAMP 継続的モニタリング戦略ガイドが要求するすべての報告は、FedRAMP 情報システムセキュリティ責任者 (ISSO:Information System Security Officer) へ提供される。これらは FedRAMP TR (DoD 職員を含む) によって審査され、必要に応じて JAB によって承認される。

DoD の継続的な監視要件は FedRAMP のものと同じであるが、FedRAMP+ C/CE のすべての報告書および成果物は、この情報に関する DoD と CSP の唯一の連絡先として DISA AO の担当者に直接提供される。DISA は、ミッションオーナー、AO、サイバーセキュリティ・サービス・プロバイダ (CSSP: Cybersecurity Service Providers) と適切な継続的なモニタリング情報 (FedRAMP と FedRAMP+) を共有する。

この情報は、ミッションオーナー、AO、および DISA AO が CSO をアセスメントし、承認するために使用される。これらの評価は、ミッションオーナーのシステムの ATO と CSP の PA のそれぞれを継続する決定の通知を行う。DISA AO は、この要件に基づいて PA の撤回を検討しなければならない場合、ミッションオーナーと密接に調整を行う。

図 4 に CSP が FedRAMP JAB PA を有する場合の継続的モニタリング情報の通常の流れを示す。

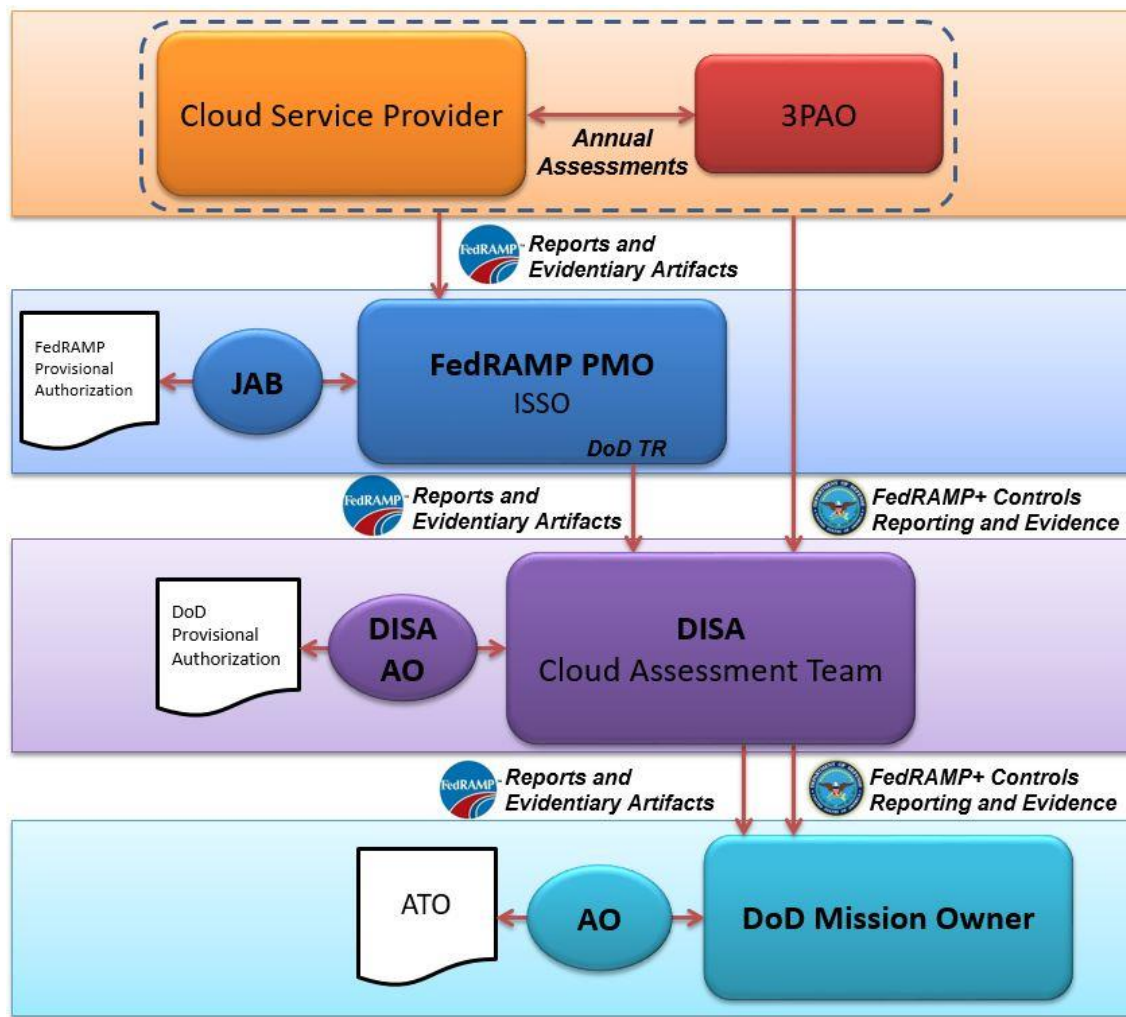


図 4 FedRAMP JAB PA を有する CSO に対する DoD の継続的モニタリング

図 5 は、CSO が FedRAMP カタログに記載されている 3PAO 非 DoD 連邦機関の ATO 保有する場合の、継続的モニタリング情報の流れを示している。FedRAMP JAB は機関の ATO を管理していないため、情報が CSP から FedRAMP PMO に流れることはない。

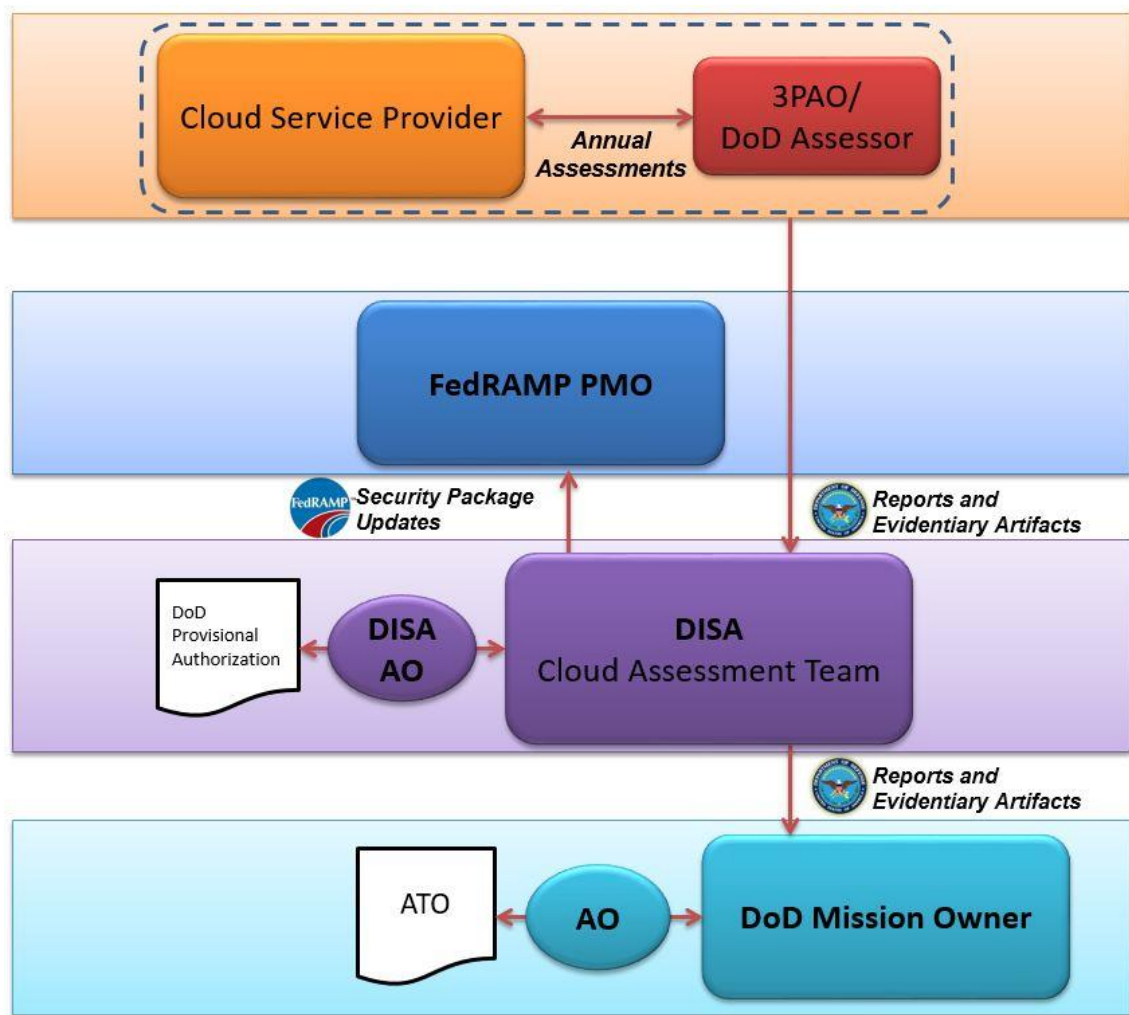


図 5 3PAO で評価された非 DoD 連邦機関 ATO による FedRAMP CSO の DoD 継続的モニタリング

5.3.1.2 DoD で評価された CSO の継続的なモニタリング

図 6 は、DoD PA と ATO を持っているが、FedRAMP カタログにない DoD のプライベート／コミュニティ CSO の継続的モニタリングの情報の流れを示している。継続的なモニタリングは、FedRAMP 継続モニタリング戦略ガイドではなく、DoD RMF によって指示される。RMF 認可プロセスの一環として、CSP はシステムセキュリティ計画の DoD 要件を満たす継続的なモニタリング戦略の作成を行う。その継続的なモニタリング戦略によって必要とされるすべてのレポートおよび成果物は、CSP から DISA へ提供される。DISA は、第 6 章「サイバー空間防衛とインシデントレスポンス」で定義されている CSO、DISA AO、およびサイバー・セキュリティ・サービスプロバイダ (CSSP) エンティティを利用して、これらの成果物をすべてのミッションオーナーへ配布する。

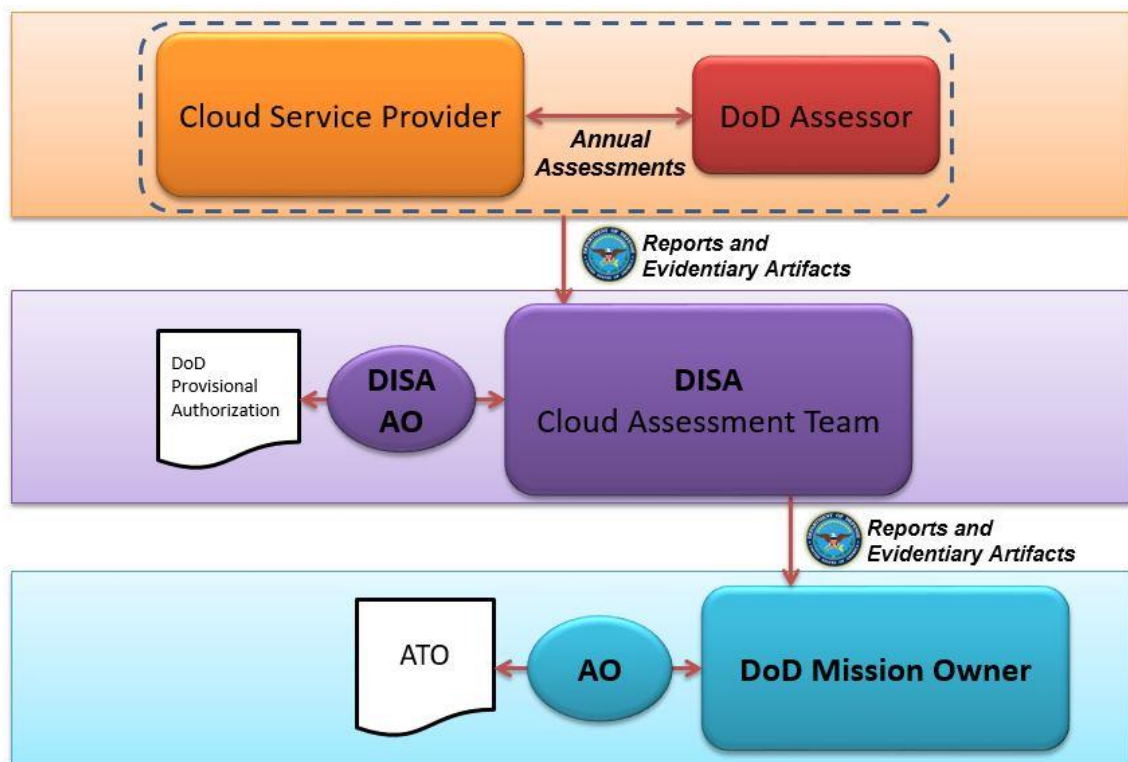


図 6 DoD がアセスメントした CSO に対する継続モニタリング

5.3.2 変更管理

CSO の DoD 変更管理プロセスは、DoD PA やホステッドミッションシステム／アプリケーションや情報のセキュリティにどのような変更が影響するかに焦点を当て、FedRAMP の内容を反映している。

2014 年 6 月 6 日付の FedRAMP 継続的モニタリング戦略ガイドは次のように述べている。

「システムはダイナミックであり、FedRAMP はすべてのシステムが常に変化していることを想定している。構成管理および変更管理プロセスは、CSP のアーキテクチャの安全なベースライン構成を維持するのに役立つ。日々の日常的な変更は、構成管理計画で説明されている CSP の変更管理プロセスによって管理される。

ただし、計画された重要な変更が行われる前に、CSP は、変更がシステムのセキュリティに悪影響を与えるかどうかを判断するために、管理策 C-4 と一致するセキュリティ影響分析を実行する必要がある。セキュリティ影響分析は、CSP の構成管理計画で説明されているように、CSP の変更管理プロセスの標準的な部分である。」

FedRAMP の場合と同様に、CSP は重要な変更が行われる前に DoD へ 30 日前に通知する必要がある。承認なしでシステムのリスク状態に影響を与える変更が行われた場合、DISA A0 は DoD の PA を取り消すことができる。継続的モニタリングの場合と同様に、CSP の変更管理プロセスは、FedRAMP カタログに含まれているかどうか、DoD で PA または ATO と評価されているかどうかによって異なる。図 7、図 8、および図 9 に、これらの変更管理プロセスを示す。

注：NIST SP 800-37 改訂 1、付録 F 2010 年 2 月⁵⁴は、「情報システムのセキュリティ状態に影響を与える可能性のある変更」という重要な変更を次のように定義している。「重要な変更例えば、(i) 新規またはアップグレードされたオペレーティングシステム、ミドルウェアコンポーネント、またはアプリケーションのインストール、(ii) システムポート、プロトコル、またはサービスの変更。(iii) 新しいまたはアップグレードされたハードウェアプラットフォームのインストール。(iv) 暗号モジュールまたはサービスの変更。(v) セキュリティ管理の変更。運用環境の重大な変更の例には、例えば、次のようなものがある。(i) 新しい施設への移動。(ii) 新しいコアミッションまたはビジネス機能の追加。(iii) 組織が脅威の対象となっていることについて、特定の信頼できる脅威情報の取得。(iv) 新しい／変更された法律、指令、方針、または規制の確立。

対応するセキュリティ管理：CM-3、CM-4、CA-6

5.3.2.1 DoD PA と FedRAMP カタログの CSO の変更管理

FedRAMP 継続的モニタリングガイドは、承認された PA の範囲の変更または CSO の認可の境界への影響としての重要な変更を定義している。CSP は、FedRAMP 継続モニタリング戦略ガイドで定義されている手順に従い、FedRAMP の重要な変更セキュリティ影響分析書⁵⁵を FedRAMP PMO に提出する。重大な変更によるセキュリティの影響のレビューは、図 7 に示すように、複数のレイヤーで実行される。計画された変更は、FedRAMP ISSO や JA の技術代表者 (TR: Technical Representatives) によってレビューされ、承認のために JAB へ転送される。同時に、DoD JAB TR は DISA に通知し、DISA は第 6 章「サイバー空間防衛とインシデントレスポンス」で定義されている CSO、DISA A0 および CSSP エンティティを利用してすべてのミッションオーナーへ通知を行う。FedRAMP ISSO のレビュー中、DoD JAB TR は DoD 関係者からのコメントを収集し、計画された変更が DoD クラウド顧客の CSO によってホストされている情報のセキュリティに悪影響を与えるかどうかを FedRAMP ISSO に通知する。

⁵⁴ NIST SP 800-37: <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>

⁵⁵ Significant Change Form:
https://www.fedramp.gov/files/2015/03/Significant_Change_Form_110812.doc

DoD は、DoD の FedRAMP+ C/CE への影響に関する変更の承認または懸念について、CSP とその 3PAO と直接連絡することがある。

FedRAMP は、重要な変更が実施され、対応するセキュリティ評価報告書が作成された後、3PAO によってセキュリティアセスメントが実施されることを要求している。CSP はまた、DoD の要件を満たすために、変更後のアセスメントにすべての FedRAMP+ C/CE を含める必要がある。DISA は影響を受けたミッションオーナーに提案された重要な変更を通知し、CSO PA の範囲内で変更の評価を提供する。ミッションオーナーは、SLA の範囲内における影響について、提案された変更の影響を評価する責任を有している。

図 7 は、CSP に FedRAMP JAB PA を有する場合の重要な変更情報の通常の流れを示す。

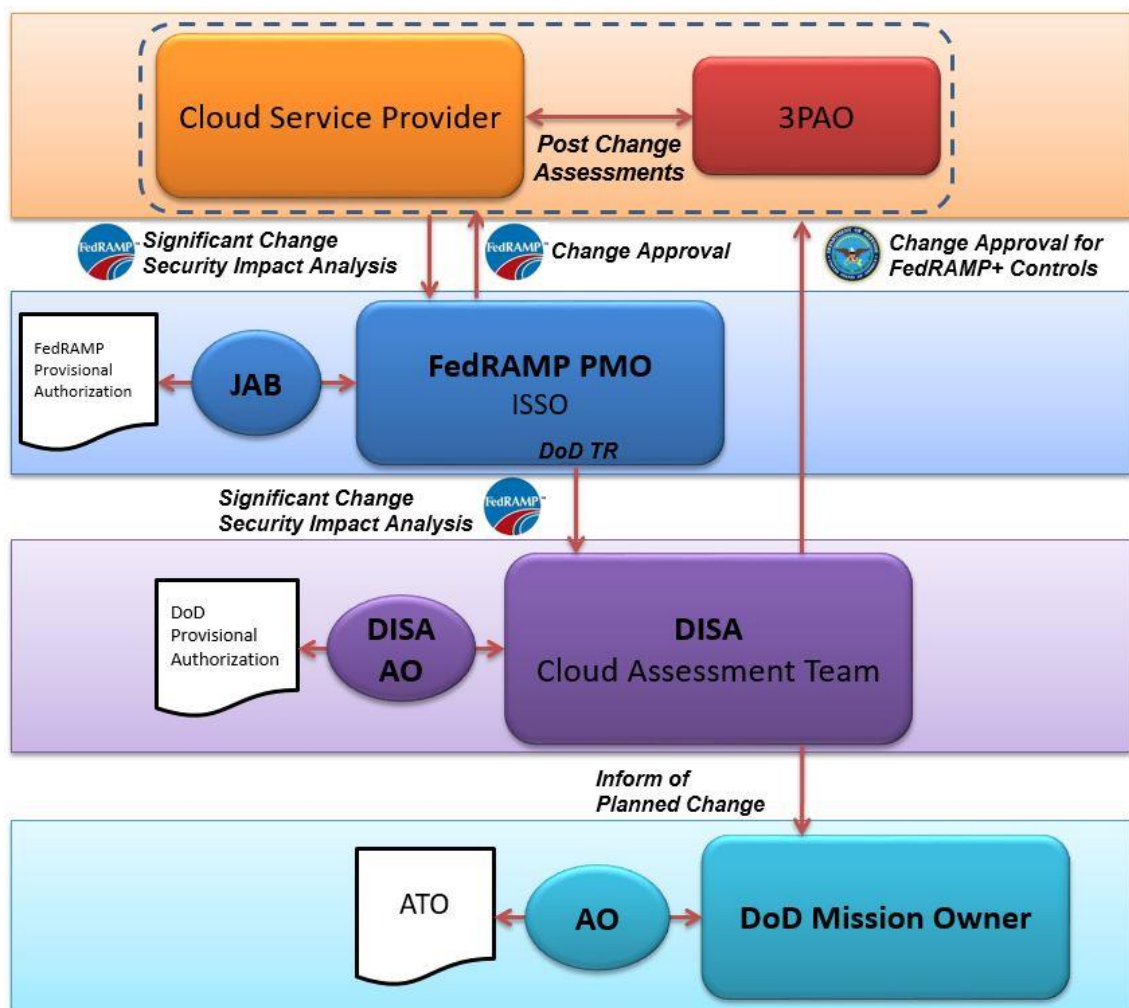


図 7 FedRAMP JAB PA を使用した CSP CSO の DoD 変更管理プロセス

DoD PA を持つ CSO が FedRAMP カタログに含まれているが JAB PA を持たない場合、CSP は他の必要な連絡先に加えて DISA へ直接通知する。(例えば、DoD 機関以外の ATO のある CSP は、その機関と DISA の両方に通知する)。これは、FedRAMP JAB が機関の ATO をコントロールしておらず、情報が CSP から FedRAMP の PMO と DISA に流れないために必要である。DISA は、CSO、DISA AO、および CSSP エンティティを使用しているすべてのミッションオーナーに、第 6 章「サイバー空間防衛およびインシデントレスポンス」で定義されているように通知を行う。セキュリティ影響分析は、FedRAMP+ C/CE をさらにカバーする必要がある。いったん通知されると、DISA は提案された変更をレビューして、DoD 情報ネットワーク (DoDIN) 全体または DISN のセキュリティに影響を及ぼすか否かを、それが認定された影響レベルにおいて評価を行う。FedRAMP セキュリティ・パッケージのアップデートは DISA に転送される。

DoD は、FedRAMP と同様、重要な変更が実施された後、対応するセキュリティ評価報告書が作成された後、3PAO によってセキュリティ評価が実施されることを要求している。CSP はまた、DoD 要件を満たすために、変更後の評価にすべての FedRAMP+ C/CE を含める必要がある。DISA は影響を受けたミッションオーナーに提案された重要な変更を通知し、CSO PA の範囲内で変更の評価を提供する。ミッションオーナーは、SLA の範囲内にある影響の提案された変更の影響を評価する責任がある。

図 8 は、CSO が FedRAMP カタログに記載されている 3PAO 非 DoD 連邦政府機の ATO を有する場合の重要な変更情報の通常の流れを示している。FedRAMP JAB は機関の ATO をコントロールしていないため、CSP からの情報は認定機関から FedRAMP PMO に流れることはない。DoD へ潜在的な変更が届かない可能性を避けるため、CSP は認定当局に加えて DISA に変更要求を送信する必要がある。

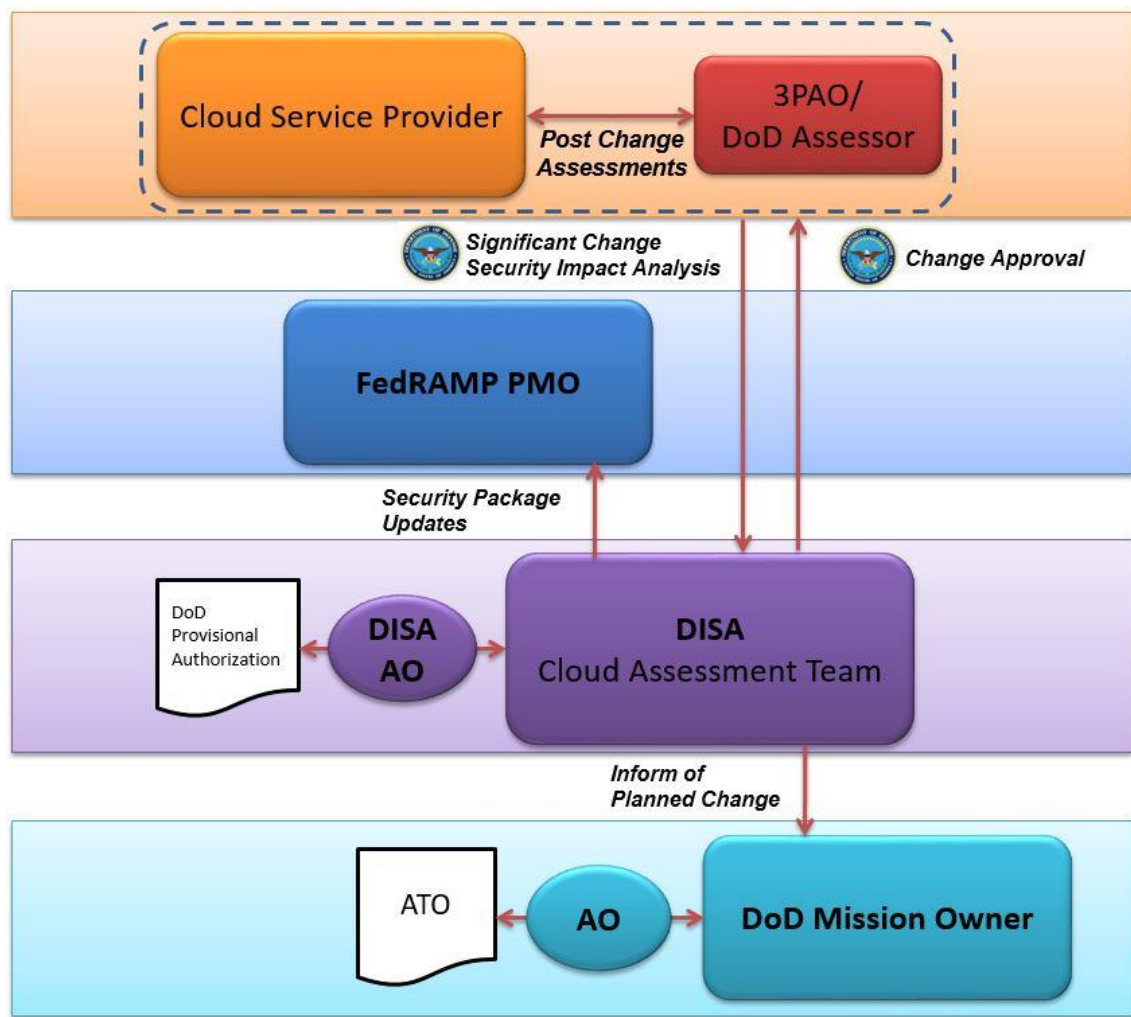


図 8 3PAO 評価された連邦機関 ATO をもつ CSO に対する DoD 変更管理プロセス

5.3.2.2 DoD で評価された CSO の変更管理

図 9 は、DoD SCA 組織によって評価され、DoD AO によって認可された DoD PA または ATO を有する非 FedRAMP CSO の重要な変化の流れを示す。重要な変更情報のレビューは、FedRAMP の変更制御プロセスではなく、DoDRMF によって指示される。CSP は同様の責任を有するが、DISA に直接報告する。DISA は、第 6 章「サイバー空間防衛とインシデントレスポンス」で定義されている CSO、DISA AO、および CSSP エンティティを利用して、これらの成果物をすべてのミッションオーナーに配布する。これらのエンティティは、提案された変更をレビューして、PA または ATO に関する CSO のセキュリティの態勢に悪影響を及ぼさないことを保証する。計画された変更は、CSO の具体的な使用に関して、CSO を利用しているミッションオーナーが見直すことになる。

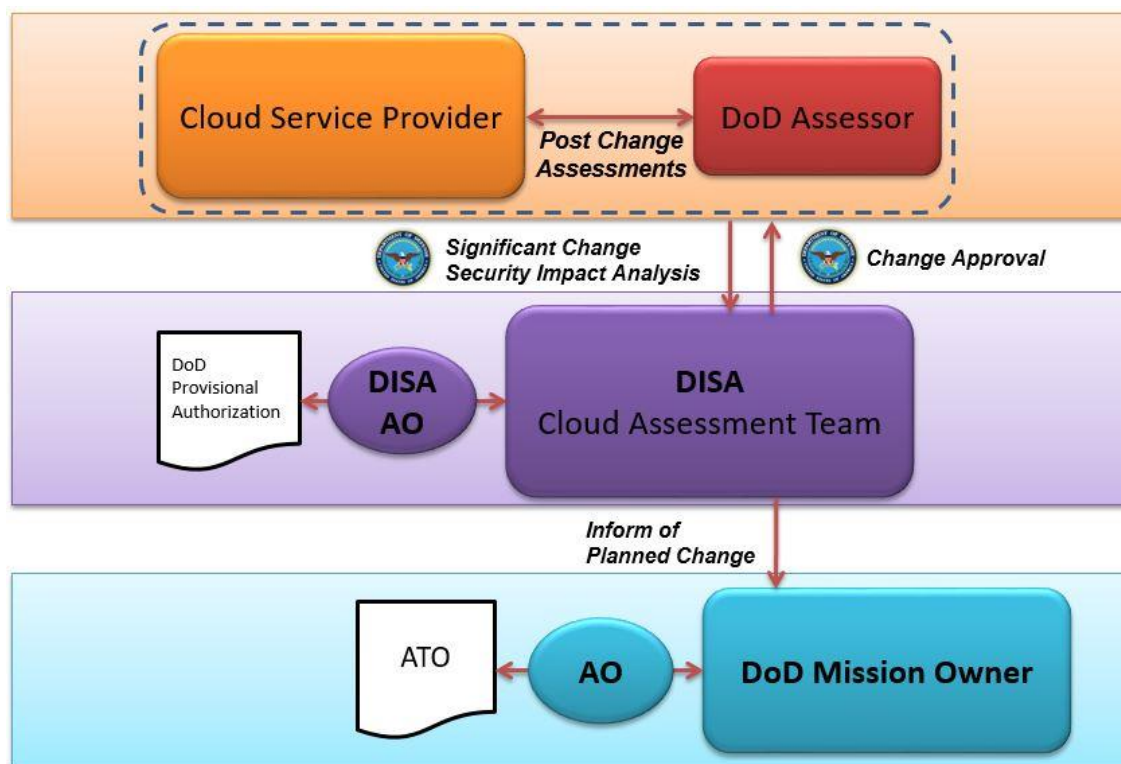


図 9 DoD 自己評価 CSP/CSO の DoD 変更管理プロセス

5.4 クラウドサービス提供者の DoD 公開鍵基盤(PKI)の利用

FedRAMP の IA-2(12)では、「情報システムが個人身分証明書 (PIV:Personal Identity Verification) 資格情報を受け入れて電子的に検証する」と規定している。また FedRAMP 補足ガイダンスでは、「共通アクセスカード(CAC:Common Access Card) (すなわち DoD が実装した PIV/FIPS 201/HSPD-12) を含む」としている。CSP は DoD エンティティの認証のために、DoD PKI の利用に対応しなければならない。(例えば、CSO の設定に DoD や連邦政府のミッションオーナーの特権ユーザがログインする Web ポータル)

以下のセクションでは、CSP がどのように責任を果たしているかについて、補足のサブセクションで詳しく説明する。

影響レベル 2: エンティティの認証やホストされている DoD 情報システムの特定に CSP が責任を負う場合、CSP は DoD 8520.03 に従って DoD PKI 証明書を使用する。CSP は、DoD 特権ユーザの認証に「共通アクセスカード (CAC : Common Access Card)」または「Alt トークン」と呼ばれる物理トークンの使用を強制する。CSP は、DoD 証明書および DoD 認証局の失効を確認するために、DoD オンライン証明書ステータスプロトコル (OCSP : Online

Certificate Status Protocol) または証明書失効リスト (CRL: Certificate Revocation List) リソースを使用する必要がある。暗号鍵の管理と保護のために、DoD の指示と業界のベストプラクティスに従わなければならない。

影響レベル 4/5: エンティティの認証やホストされている DoD 情報システムの特典に CSP が責任を負う場合、CSP は DoD 8520.03 に従って DoD PKI 証明書を使用する。CSP は、DoD 特権ユーザおよび DoD 非特権ユーザの認証に「共通アクセスカード (CAC)」または「Alt トークン」と呼ばれる物理トークンの使用を強制する。CSP は、DoD 証明書および DoD 認証局の失効を確認するために、DoD OSCP または CRL リソースを使用する必要がある。暗号鍵の管理と保護のための DoD の指示と業界のベストプラクティスに従わなければならない。DoD 発行の PKI サーバー証明書は、DoD の利用専用として契約された CSP の DoD 顧客注文/サービス管理ポータルと SaaS アプリケーションおよびサービスを識別するために使用される。

影響レベル 6: オンプレミス CSO が DoD エンティティの認証やホストされている DoD 情報システムの識別を担当する場合、CSP は DoD 8520.03 および CNSSP-25 に従って NSS PKI 証明書を使用する。CSP は、DoD ミッションオーナーと CSP 特権ユーザおよび非特権ユーザの認証に CNSS Secret Internet Protocol Router Network (SIPRNet) ハードウェアトークンと呼ばれる物理トークンの使用を強制する。NSS PKI を実装する場合、CSP は NSS 証明書および NSS 認証局の失効を確認するために NSS OSCP または CRL リソースを使用する必要がある。暗号鍵の管理と保護のために CNSS/NSA の指示に従わなければならない。CNSS 発行の PKI サーバー証明書は、DoD の利用専用として契約された CSP の DoD 顧客注文/サービス管理ポータルと SaaS アプリケーションおよびサービスを識別するために使用される。

注: CSP は、レベル 4 以上の全般的な DoD ユーザアクセスに対して、すべてのサービス提供のためのカスタマー発注/サービス管理ポータルと、必要な PKI との統合を可能にする顧客構成可能なサービスを提供する必要がある。コンプライアンスを完全にするために、CSP はレベル 2~5 の DoD PKI および連邦 PKI と統合する。レベル 6 では CSP が NSS (SIPRNet) PKI と統合される。DoD と NSS の両方の PKI は DISA⁵⁶によって運用され、連邦 PKI は GSA によって運用されている⁵⁷。PK 対応の顧客注文/サービス管理ポータルでは、連邦政府の要件を満たすために、CSP が最もよく決定する個別の URL または専用アプリケーション/アプリケーションインターフェースが必要になる場合がある。

関連する管理策: IA-2 (1)、IA-2 (2)、IA-2 (3)、IA-2 (8)、IA-2 (11)、IA-2 (12)、IA-5 (2)、IA-5 (11)、IA-7、IA-8

⁵⁶ DoD PKI/PKE: <http://iase.disa.mil/pki-pke/Pages/index.aspx>

⁵⁷ Federal PKI: <http://www.idmanagement.gov/federal-public-key-infrastructure>

注：オンプレミス・レベル 6 の CSP および CSO の NSS PKI および SIPRNet トークン要件は、OUSD (I) および DSS と調整する必要がある。関連するポリシーについては、前述のセクション 4.2 「DoD クラウドサービスとエンタープライズサービスアプリケーションのアセスメント」における影響レベル 6 のトピックスで説明している。DoD レベル 6 暫定認証のためのオンプレミス CSP およびその CSO のための調整されたガイダンスおよび要件は、CC SRG の将来のリリースで規定される可能性がある。この注釈は、セクション 5.4 のすべてのサブセクションに適用される。

5.4.1 識別、認証、アクセス制御資格情報

DoD 8520.03 「情報システムの身元認証」は、DoD の特権ユーザおよび非特権ユーザがアクセスを許可される前に、DoD の情報システムに対して身元を確認するために使用する必要がある資格情報を定義する DoD のポリシーである。また、DoD 情報システムが互いに識別するために使用する資格情報も定義している。これは、クラウドサービスでインスタンス化された DoD の情報システムに完全に適用される。さらに、CNSS Policy #25 および CNSSI 1300 は、NSS の同様のガイダンスを提供している。この議論の目的のために、識別および認証のプロセスを I&A と呼ぶ。

5.4.1.1 CSP とミッションシステムインターフェースのミッションオーナー クレデンシャル

このセクションでは、以下のカテゴリの DoD 8520.03 に基づいて、各情報への影響レベルが必要とされるミッションオーナーのアクセス制御資格を定義している。

- ミッションオーナーCSP の顧客発注およびサービス管理インターフェースまたはポータル（すべてのサービス提供 (IaaS/PaaS、SaaS)）に対する特権ユーザのアクセス。
 - DoD PKI との統合は、通常 CSP の責任である。最低限、CSP は、ミッションオーナーが DoD PKI と統合する CSP サービスを構成できるようにする機能を提供する責任がある。
- ミッションオーナーCSP SaaS サービスへのアクセス権が特権のないユーザ（ミッション・アプリケーションエンドユーザ）。
 - DoD PKI との統合は、通常 CSP の責任である。最低限、CSP は、ミッションオーナーが DoD PKI と統合する CSP サービスを構成できるようにする機能を提供する責任がある。
- IaaS/PaaS でインスタンス化されたミッションオーナーのシステムとアプリケーションに対する特権のないユーザアクセス。（すなわち、ミッション・アプリケーションのエンドユーザ）
 - 実施はミッションオーナーの責任である。

- ミッションオーナーの管理および保守の目的で、IaaS/PaaS でインスタンス化されたシステムおよびアプリケーションへの特権ユーザのアクセス。
 - 実施はミッションオーナーの責任である。

表 4 に、様々な利用形態に対して各影響レベルで必要とされるミッションオーナー資格のタイプと、それらが必要とされるポリシーを示す。DoD Policy 列には、ミッションオーナーが CSP の CSO でインスタンス化するシステムおよびアプリケーションで使用するために実装する必要がある認証方法が示されている。これは主に IaaS/PaaS に適用される。IA2 (12) 欄は、CSP が DoD 顧客に提供するサービスで使用するために実装する必要がある認証方法を示している。これは主に、SaaS および CSP の顧客注文/サービス管理ポータルに適用される。

表 4 ミッションオーナー資格

影響レベル	DoD ポリシーに従ったミッションオーナーによる実装	FedRAMP IA-2(12)に従った CSP による実装
レベル 2	<ul style="list-style-type: none"> ・ 一般に公開された情報への特権を持たないユーザのアクセスには、情報の所有者が要求しない限り、I&A は必要とされない。必要に応じて、ミッションオーナーは、使用する I&A のタイプを決定する。 ・ 公開されていない非 CUI および重要でないミッション情報への非特権ユーザアクセスには、DoD の文字数と複雑さの要件を満たすユーザ識別子 (UID:User Identifier) およびパスワードを使用した最低限の I&A を必要とする。ミッションオーナーは、個人情報の重要度に応じてより強力な I&A 技術 (例えば、2 ステップ認証を伴う UID/パスワード、ワンタイムパスワード 	<ul style="list-style-type: none"> ・ 非公開でリリースされた非 CUI および非クリティカルミッション情報への非特権ユーザのアクセスには、少なくとも DoD の文字数と複雑さの要件を満たすユーザ識別子 (UID) およびパスワードを使用した I&A が必要である。ミッションオーナーは、個人情報の重要度に応じてより強力な I&A 技術 (例えば、2 要素トークンをベースとしたワンタイムパスワード、DoD 承認の⁵⁸PKI トークン/証明書など) の適用を要求することが奨励される。

⁵⁸ DoD-approved PKIs: <http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx>

	<p>に基づく 2 要素トークン、DoD 承認の PKI トークン／証明書、CAC/PKI など)の適用を要求することが奨励される。</p> <p>・ IaaS/PaaS でインスタンス化されたミッションオーナーのシステム／アプリケーションを管理するためのミッションオーナーの特権ユーザのアクセスには、DoD CAC/PKI または Alt Token/PKI を使用する必要がある。</p>	<p>・ミッションオーナーの特権ユーザは、すべてのサービス提供のための CSP の顧客注文／サービス管理ポータルへのアクセスには、DoD CAC/PKI または Alt Token/PKI を使用する必要がある。</p>
レベル 4 および 5	<p>・ CUI、非 CUI クリティカルミッションデータや非格付け NSS (L5) への非特権ユーザアクセスには、DoD CAC/PKI またはその他の DoD 承認の PKI⁵⁹を使用する必要がある。</p> <p>・ IaaS/PaaS でインスタンス化されたミッションオーナーのシステム／アプリケーションを管理するためのミッションオーナーの特権ユーザのアクセスには、DoD CAC/PKI または Alt Token/PKI を使用する必要がある。</p>	<p>・ CUI、非 CUI クリティカルミッションデータや CSP の SaaS 製品の非格付け NSS (L5) 情報への非特権ユーザアクセスには、DoD CAC/PKI またはその他の DoD が承認した PKI⁶⁰を使用する必要がある。</p> <p>・ミッションオーナーの特権ユーザが、すべてのサービス提供のために CSP の顧客注文／サービス管理ポータルにアクセスするには、DoD CAC/PKI または Alt Token/PKI を使用する必要がある。</p>
レベル 6	<p>・ 格付け情報への非特権ユーザのアクセスには、NSS SIPRNet Token / PKI の使用が必要である。</p> <p>・ IaaS/PaaS でインスタンス化されたミッションオーナーのシステム／アプリケーションを管理する</p>	<p>・ CSP の SaaS 製品で格付けされた情報への非特権ユーザのアクセスには、NSS SIPRNet Token/PKI を使用する必要がある。</p> <p>・ミッションオーナーの特権ユーザが、すべてのサービス提供のために CSP の顧客注文／サービス管理ポ</p>

⁵⁹ DoD-approved PKIs: <http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx>

⁶⁰ DoD-approved PKIs: <http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx>

	ミッションオーナーの特権ユーザのアクセスには、NSS SIPRNet トークン/PKI を使用する必要がある。	タルにアクセスするには、NSS SIPRNet Token/PKI を使用する必要がある。
--	---	---

注：CSP のサービス提供の一部を管理することに関与、または CSP からサービスを注文することができる（すなわち、CSP の顧客注文およびサービス管理インターフェースまたは、サービス提供のためのポータル（IaaS/PaaS、SaaS）のアカウントを保持）ミッションオーナーの要員は、DoD の特権ユーザとみなされるため、DoDI 8520.03 に従って DoD CAC または Alt Token を使用して認証する必要がある。

注：一部のレベル 4/5 システムでは、CUI（例えば PII/PHI）にアクセスする権限があるが、DoD CAC/PKI またはその他の DoD が承認した PKI 認証を受け取ることができない非特権ユーザ（例：退職者）をサポートする必要があることが認識されている。このような場合、ミッションオーナーは、そのようなデータを非格付な重要度レベル 1 と位置づけ、DoDI 8520.03 に従った認証強度 A（認証にパスワード）の使用を可とした A0 の承認を求める。そのような対象は通常、DoD のパスワードポリシーに従って、UID と強力なパスワードを使用する必要があるが、Web サイトまたは UID/パスワードの組み合わせを入力した後のアプリケーションとは別の通信パスを使ってアクセスコードをユーザへ送るなど、ミッションオーナーは、より強力な 2 段階の検証を実装することが推奨される。実際には、これは 2 要素認証システムになる。

5.4.1.2 CSP 特権ユーザの資格情報

このセクションでは、ミッションオーナーのシステムをサポートする CSP のインフラストラクチャを管理するときに CSP 特権ユーザが使用する必要がある I&A とアクセス制御の資格情報を定義している。

影響レベル 2/4：セクション 5.2.2.1「影響レベル 2 場所と分離の要件」、5.2.2.2「影響レベル 4 場所と分離の要件」、および FedRAMP の IA-2(1) と IA-2(3) で説明されたレベル 2 と 4 の分離要件に従って、CSP は、連邦および DoD の契約サービスをサポートする CSP インフラストラクチャを管理および維持するために、最低限 CSP 特権ユーザアクセスに対し、2 要素の認証を実装する必要がある。DoDI 8520.03 証明書強度 D と同様の多要素のワンタイムパスワードまたは PKI 証明書テクノロジーソリューションを実装するハードウェアトークン技術を使用するベストプラクティスが望ましいが、これらの ID 資格情報は最低限 DoDI 8520.03 証明書強度 C と同様のマルチトークンソリューションまたは多要素タワンタイムパスワードを利用する。

影響レベル 5 : セクション 5.2.2.3 「影響レベル 5 場所と分離の要件」と DoD のポリシーで説明されているレベル 5 の分離要件に従って、維持管理を行うために CSP の特権ユーザが、CSP 専用の連邦および DOD の契約サービスをサポートするためのアクセスに対し、強力な 2 要素の I&A を実装しなければならない。これらの資格情報は、最低限でも多要素ワンタイムパスワードを実装したハードウェアトークン技術、または DoDI8520.02 証明書強度 D と同様な PKI 証明書テクノロジーソリューションを用いなければならない。

注 : DoDI 8520.03 では、DoD システムへの特権アクセスには、DoD またはパートナー管理システムのすべての管理者が資格証明書の強度 E (連邦機関、連邦 PKI ポリシー当局プログラムの下で認可された共有サービスプロバイダ、または DoD CIO によって証明書の強度 E として、特別に許可された資格証明書プロバイダ (例えば DoD CAC または ALT) などの資格証明書サービスプロバイダから発行されたハードウェアトークン PKI 技術) を要求しているが、DoD は現時点では、CSP の資産を管理している CSP インフラストラクチャの管理者／特権ユーザに対し、この要件を強制していない。

影響レベル 6 : セクション 5.2.2.4 「影響レベル 6 の場所と分離の要件」および CNSS ポリシーで説明されているレベル 6 の分離要件を満たすため、SIPRNet に接続された連邦や DoD の契約におけるレベル 6 のサービスをサポートしている専用の CSP インフラストラクチャを維持・管理する CSP の特権ユーザによるアクセス用には、SIPRNet トークン／PKI 認証を実装する必要がある。

5.4.2 公開鍵 (PK) の有効化

公開鍵 (PK) の有効化とは、ホストとアプリケーションが以下の目的で PKI 証明書を保持または使用できるようにするプロセスを示す。

- 自分自身を他のホストでの識別
- 安全な通信経路の確立
- システム認証とユーザ認証のための DoD PKI 証明書の受け入れ
- DoD OCSP レスポンダリソースや CRL リソースを使用しながら、PKI 証明書の妥当性検証

IASE Web サイトの公開鍵インフラストラクチャ (PKI:Public Key Infrastructure) および公開鍵有効化 (PKE:Public Key Enabling) ⁶¹では、CSP の IaaS/PaaS 製品、CSP の SaaS 製品およびサービスの注文／管理ポータル／インターフ

⁶¹ DoD PKI/PKE: <http://iase.disa.mil/pki-pke/Pages/index.aspx>

ケース上にインスタンス化された PK 対応のミッションオーナーのシステム／アプリケーションに必要な情報を提供している。

5.5 方針、指針、運用上の制約事項

CSP は、DoD 固有の方針、指針、運用上の制約に適切に従わなければならない。DISA は、ケースバイケースで、特定のセキュリティ管理策、SRG、または STIG 要件と CSP 提出の同等性の評価を行う。

5.5.1 SRG/STIG コンプライアンス

ミッションオーナーは、すべてのレベルで CSP の IaaS と PaaS でインスタンス化されたすべてのミッションオーナーのシステムとアプリケーションを保護するために、適用可能なすべての DoD SRG と STIG を使用する必要がある。

CSP の CSO は、FedRAMP が選択した SP 800-53 セキュリティ管理策 CM-6 に従う。これは、IaaS、PaaS、SaaS のいずれであっても、CSP の CSO を構成しサポートするすべてのインフラストラクチャ、ハードウェアおよびソフトウェアに適用される。CSO は、FedRAMP 値で指定されたセキュリティ構成チェックリストに従って FedRAMP のもとで評価される。

すべての STIG と SRG は、SRG/STIG の適用性ガイド⁶²と共に DISA の IASE ウェブサイト⁶³で公開している。

DoD は、DoD システムをサポートするシステムの CM-6 ベースライン設定要件を満たすために、CSP が STIG や SRG を使用することを推奨している。

影響レベル 2 : CSP による STIG および SRG の使用が推奨されるが、インターネットセキュリティセンター (CIS: Center for Internet Security) ベンチマークによって提供されるような業界標準のベースラインは、STIG や SRG の代替として受け入れられる。

影響レベル 4/5/6 : CSP が STIG で言及した製品を利用するならば、STIG を適用できる。STIG に対応した製品が利用できない場合、STIG の代わりに SRG が適用される。ただし、STIG または SRG が使用可能かどうかにかかわらず、SP 800-53 管理策が適用さ

⁶² SRG/STIG Applicability Guide:

<http://iase.disa.mil/stigs/agct/Pages/index.aspx>

⁶³ STIGs and SRGs: <http://iase.disa.mil/Pages/index.aspx>

れる。CM-6 の DoD レベル 4/5/6 の値は、DoD SRG と STIG を該当するものとして利用することになるが、DISA は、CSP の商用同等品（CIS ベンチマークなど）の使用状況をケースバイケースで評価する。

DoD テナントのみを提供する専用インフラストラクチャの場合、CSP はすべての DoD STIG や SRG を利用して、契約されているすべての DoD クラウド・コンピューティング・サービスを保護する必要がある。これは、IaaS、PaaS、および SaaS 製品のレベル 4 以上に適用される。

対応するセキュリティ管理策：CM-6

5.6 物理的設備及び人的要件

以下のセクションでは、影響レベルに合わせて施設と要員の要件について説明している。

5.6.1 施設要件

影響レベル 2：レベル 2 の情報をサポートする CSP のデータ処理施設は、FedRAMP ベースライン中で定義されている物理的セキュリティ要件を満たすこと。

影響レベル 4/5：レベル 4 および 5 の CSO/情報をサポートする CSP データ処理施設は、物理的セキュリティに関連する FedRAMP ベースライン中および FedRAMP+ C/CE で定義された物理セキュリティ要件を満たすこと。

影響レベル 6：クラウドサービスのインフラストラクチャおよび格付けされたサービスの提供をサポートする DoD データのオンプレミス処理施設は、情報の最高格付けレベルに見合うオープンストレージ用に設計、構築、承認された施設（セキュリティ保護された部屋として指定）に収容され、DoD 5200.01 第 3 巻「DoD 情報セキュリティプログラム：格付けされた情報の保護」⁶⁴に定義に従って、保存、処理、または送信されること。

5.6.2 CSP 要員の要件

クラウドオペレーションのコンセプトは、複数の組織間で共有されている責任と、このスペース内で適用されている先進技術とを考慮すると、人的セキュリティ要件に影響を与える可能性がある。CSP の職員が、プロビジョニングされて提供されたセキュリティ管理策／環境を変更し、提供されたシステム／アプリケーション／データ処理のセキュリティを変更する能力は、CSP によって使用されるプロセス／管理策によって異なる場合がある。

⁶⁴ DoDM 5200.01 Vol13:
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol13.pdf

CSPによって提供される基礎となるインフラストラクチャのコンポーネント（ハイパーバイザ、ストレージサブシステム、ネットワークデバイスなど）およびサービスのタイプ（IaaS、PaaS、SaaS など）は、CSP がアクセスを決めることになるが、CSP の職員が DoD ミッションやデータで問題を発生させるリスクがある。CSP の要員は、一般的に、知る必要性(need-to-know)の理由で、公開のために承認された情報を除いて、顧客データ／情報へのアクセスが承認されていないが、職務を通じて情報にアクセスできると考えられている。レベル 2 以上のさまざまなレベルでの DoD の情報へのアクセスは、国籍によって制限されている。米国市民または非市民である米国籍は、8 U.S. Code § 1408⁶⁵号で定義されているように、国の所属は 22 CFR 120.15⁶⁶ - 米国人および 120.16 - 外国人で定義されている。

情報影響レベルによる制限は次のとおりである。

影響レベル 2: DoD の公開情報を処理／保存するシステムにアクセスできる CSP の要員は、米国市民、米国籍、米国人、または外国人である。すなわち、制限はない。

影響レベル 4/5: 影響レベル 4/5 で DoD CUI 情報または情報自体を処理／保存するシステムにアクセスできる CSP 要員は、米国市民、米国籍、または米国人でなければならない。外国人はアクセスできない。

影響レベル 6: 格付けされた情報を処理／保存するシステムへのアクセス権を持つ CSP 要員または情報自体は、米国市民でなければならない。

対応セキュリティ管理策：PS-2、PS-3

5.6.2.1 CSP 要員の要件 PS-2: 職位の分類

FedRAMP のベースライン中(moderate)には、人的セキュリティ管理策 PS-2、PS-3、および強化 PS-3 (3) が含まれている。PS-2 の下では、CSP は「すべての組織ポジションにリスク指定を割り当てる」と「それらのポジションを満たす個人のスクリーニング基準を確立する」ことが求められている。補足ガイダンスでは、「ポジションリスク指定は、人事管理オフィス (OPM: Office of Personnel Management) の方針およびガイダンスを反映している」としている。OPM ポジション指定プロセスは、職務、監督レベル、および違法行為が影響を及ぼす可能性のある範囲（すなわち、政府機関全体、複数の機関、または機関）が考慮される。

⁶⁵ 8 U.S. Code § 1408: <https://www.gpo.gov/fdsys/pkg/USCODE-2010-title8/pdf/USCODE-2010-title8-chap12-subchapIII-partI-sec1408.pdf>

⁶⁶ CFR 120.15, 120-16: <https://www.gpo.gov/fdsys/pkg/CFR-2011-title22-vol1/pdf/CFR-2011-title22-vol1-sec120-15.pdf>

IT システムおよび情報アクセスについては、アクセスされる情報の感度レベル（すなわち、CUI 以外、CUI および格付けされたもの）も考慮される。

連邦機関が、国家安全保障の職位（例えば、外国の攻撃またはスパイ活動から国家の防衛に関連し、機密情報への定期的なアクセスを必要とする職位）や、パブリック・トラスト職位（例えば、インフォメーション・セキュリティ・システムの保護の責任を含む高・中のリスクレベルの職位）を決定するにあたり、組織的かつ一貫性のある手段を提供可能にするために、「OPM 職位指定システム 2010 年 10 月の文書」⁶⁷[68]および「OPM 職位指定ツール」⁶⁸が提供されている。職位のリスクレベルは、職位指定ツールを使用して決定される。職位は、機微性のレベルと最終的に必要とされるセキュリティ調査のタイプに影響を及ぼす国家安全保障とパブリック・トラストの両方の考慮事項を有する可能性がある。Position Sensitivity Tool は、主要な CSP 要員の職位の機微性、リスクレベル、調査要件を決定するために使用される。

DoD の主な関心事は、DoD の情報に直接アクセスまたはアクセスを得る能力を有する CSP 職員、情報技術の処理、保管、または送信のセキュリティに影響を及ぼす可能性のある責任を持つ CSP 職員である。OPM 方針の下では、CUI または機密情報にアクセスできるそのような人物は、「クリティカル・センシティブ」または「ハイリスク」と指定された職位に符号している。しかし、その人物の「より高い権限（例えば、「クリティカル・センシティブ」または「ハイリスク」の職位）からの技術的レビューの下で仕事を実行している場合については、その職位は「非クリティカル・センシティブ」または「中リスク」として扱われる。非 CUI および公開された情報へのアクセス権しか持たない職位は、「非センシティブ」または「低リスク」と指定することができる。すべてのポジションは、あるレベルの「パブリック・トラスト」を持っているとみなされる。

PS-2 と DoD 5200.2-R の Personnel Security Program⁶⁹カテゴリ I 自動データ処理 (ADP) (ADP-1 または IT-1) に基づく DoD ポリシーの観点からは、職位として、コンピュータセキュリティプログラムの企画、指示、実装；ハードウェアおよびソフトウェアを含むコンピュータシステムの方向性、計画および設計に大きな責任を負う；または操作やメンテナンス中に重大な障害を引き起こすリスクが比較的高い；または莫大な個人的利益を実現できるような個人を含むものである。これらの職位は、「クリティカル・センシティブ」と呼ばれて

⁶⁷ OPM Position Designation System document:
<http://www.opm.gov/investigations/backgroundinvestigations/position-designation-tool/oct2010.pdf>

⁶⁸ OPM Position Designation Tool: <http://www.opm.gov/investigations/background-investigations/positiondesignation-tool/>

⁶⁹ DoD 5200.2-R: <http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf>

いる。カテゴリ II の自動データ処理 (ADP) (ADP-2 または IT-2) の職位には、ADP-1 カテゴリのリストと同じ責任を持ち、その仕事がシステムの完全性を保証するために、ADP-I カテゴリの上位機関によって技術的にレビューされている個人を含んでいる。これらの職位は、「非クリティカル・センシティブ」に指定されている。これらの指定は、OPM 職位指定文書と自動化ツールと一致している。DoD PA を受け取るには、CSP は要員の職位カテゴリと PS-2 への準拠が、「クリティカル・センシティブ (例えば DoD の ADP-1)」、「高リスク」、「非クリティカル・センシティブ (例えば、DoD の ADP-2)」、「中リスク」、「低リスク (例えば非 CUI な公開情報だけをアクセス)」などの OPM 職位指定と同等であることを示さなければならない。これらの指定は、スクリーニングのレベルを PS-2 の後半および PS-3 に従って確立するように促す。

5.6.2.2 CSP 要員の要件 PS-3: 背景調査

PS-3 および PS-3 (3) の下では、CSP は「情報システムへのアクセスを許可する前に個人をスクリーニングする」ことが求められ、組織の定義した頻度で再スクリーニングする必要がある。PS-3 (3) は、CUI のような「特別な保護を必要とする」情報のための「追加の人員スクリーニング基準」を扱っている。

2014 年 6 月 6 日の FedRAMP Control Specific Contract Clauses v2 にある PS-3 の FedRAMP 補足ガイダンス⁷⁰によると、機関は、「OPM と OMB の要件に基づいて」、情報にアクセスできる、またはアクセスを得ることができる CPS の要員について、バックグラウンド調査の実施が規定されている。DoD について、最低限の指定は次のようにレベル毎に規定されている。

影響レベル 2: レベル 2 のクラウドサービスをサポートする CSP 要員は、人的セキュリティ要件を満たし、FedRAMP のベースライン中に従って OPM 方針で定義されているバックグラウンド調査を受ける。したがって、「非センシティブ」または「低リスク」の職位指定に基づくレベル 2 情報へのアクセス (すなわち、公開および非 CUI の重要でないミッション情報へのアクセスのみを有する職位) を有する CSP 要員に必要な最小限の背景調査は、国家機関によるチェックと問い合わせ (NACI: National Agency Check with Law and Credit) である。職位の機微性またはリスクレベルと、結果としての調査は、追加のリスク考慮事項に基づいて、ミッションオーナー/AO が決定した最小要件を超えて増強する可能性がある。例えば、情報の機密性、完全性または可用性 (CIA: Confidentiality, Integrity or Availability) が、ツールを使用して「非クリティカル・センシティブ」または「中程度のリスク」の職位に基づいていると判断された場合、「非クリティカル・センシティブな契約

⁷⁰ FedRAMP Control Specific Contract Clauses v2, June 6, 2014;
<http://cloud.cio.gov/document/control-specificcontract-clauses>

者」対し NACLC(National Agency Check with Law and Credit)または「中リスクの職位」について MBI(Moderate Risk Background Investigation)が必要となる可能性がある。

影響レベル 4/5：レベル 4 および 5 のクラウドサービスをサポートする CSP 要員は、人的セキュリティ要件を満たし、FedRAMP の中ベースライン、人的セキュリティに関連する FedRAMP+ CE、および DoD の人的セキュリティポリシーによる OPM ポリシーで定義されているバックグラウンドチェックを受ける。このように、「クリティカル・センシティブ」（例えば、DoD の ADP-1）職位指定に基づくレベル 4 および 5 の情報にアクセスする CSP 要員に必要な最小限のバックグラウンド調査は、SSBI(Single Scope Background Investigation) または BI(Background Investigation) を「高リスク」職位指定に使用することができる。DoD の ADP-2 などの「非クリティカル・センシティブ」に基づいたレベル 4 とレベル 5 の情報にアクセスできる CSP 要員のために必要な最小限のバックグラウンド調査は、NACLC による国家機関のチェック（非クリティカル・センシティブ契約者）または「中リスク」の職位指定のための MBI(Moderate Risk Background Investigation) である。

レベル 2、4、または 5 の DoD PA を受け取るには、CSP は、システムやデータへのアクセスを必要とする要員（例えば、ハイパーバイザー以上）に対し、記載されている調査要件に従わなければならない。CSP のインフラストラクチャ（例えば、ハイパーバイザー以下）にアクセスする人員は、OPM 調査要件を満たすか、または各職位の指定について、CSP のバックグラウンド調査および PS-3 と PS-3（3）が OPM の調査と一致することを CSP が証明しなければならない。

注：DoD は、カテゴリ 595 27HR サポート：就労前のバックグラウンド調査ウェブサイト⁷¹に掲載されている GSA 連邦調達サービス業者(Federal Acquisition Service Contractor)としてリストされている調査請負業者から上記のものと同等の調査を CSP が要求できるとしている。そのような請負業者を使用し、同等の調査を要求することによって、CSP は DoD PA を取得するにあたり、同等であることを実証し、契約授与後に必要な調査の準備することができる。

影響レベル 6：CNSSI 1253 格付け情報オーバーレイによって呼び出される PS-3（1）に従って、セキュアな区画、格付された情報の処理をサポートするインフラストラクチャへアクセスする人物またはパブリック・トラスト職位の適合性／調査要件（例えば、DoD ADP-1 ポジションのシステム管理者にとって好ましいと判断される SSBI）に加えて機密情報の取

⁷¹ GSA Investigation Contractors:

<http://www.gsaelibrary.gsa.gov/ElibMain/sinDetails.do?executeQuery=YES&scheduleNumber=738+X&flag=&filter=&specialItemNumber=595+27>

り扱い者には、適切なレベルでのセキュリティクリアランスが必要である。システムおよびネットワーク管理者（すなわち、特権ユーザ）は、通常、need-to-know の理由から機密情報を扱うことは認められていないが、職務を通じて機密情報にアクセスできるとみなされる。したがって、これらの要員は、保存、処理、または送信される格付け情報に対応した適切なレベルでクリアランスを要求される。

DoD 要員のクリアランスは、いずれも DoD 人員セキュリティプログラム（PSP: Personnel Security Program）と呼ばれる DoDI 5200.02⁷²および DoD 5200.2-R⁷³で定義されている DoD のプロセスを通じて許可される。商用 CSP の人員クリアランスは、産業人事セキュリティクリアランスプロセス⁷⁴によって付与される。

オンプレミスおよびオフプレミスのレベル 6 CSO の契約には、48 連邦規制コード（CFR: Code of Federal Regulations）第 4.4 項「業界内における格付けされた情報の保護」⁷⁵および連邦調達規則（FAR: Federal Acquisition Regulations）セクション 52.204-2 - 「セキュリティ要件」⁷⁶に従って、格付け情報へアクセスを必要とする請負業者に関する言語が含まれる。

レベル 6 の DoD PA を受け取るには、CSP は施設と CSO を管理する要員（トップレベルの企業経営者を含む）のクリアランスを保持するか、または、産業人事セキュリティクリアランスプロセスで定義された要求を満たすことを証明しなければならない。

オンプレミスのレベル 6 の CSO の施設および人員のクリアランスは、他の DoD 契約と同様に、契約者が格付け情報へのアクセスを必要とするか、または他の目的のために必要とされるかによって処理される。

オフプレミスのレベル 6 の CSO 施設および人員のクリアランスについては、他の防衛産業基地（DIB: Defense Industrial Base）請負業者と同様に契約プロセスを通じて処理される。このプロセスは、OUSD（I）と DSS の範中である。

⁷² DoDI 5200.2: http://www.dtic.mil/whs/directives/corres/pdf/520002_2014.pdf

⁷³ DoD 5200.2-R: <http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf>

⁷⁴ Industrial Personnel Security Clearance Process: http://www.dss.mil/psmo-i/indus_psmo-i_process_applicant.html

⁷⁵ 48 CFR Subpart 4.4:

<https://www.gpo.gov/fdsys/granule/CFR-2011-title48-vol1/CFR-2011-title48-vol1-part4-subpart4-4>

⁷⁶ FAR 52.204-2:

<https://www.gpo.gov/fdsys/pkg/CFR-2002-title48-vol2/pdf/CFR-2002-title48-vol2-sec52-204-1.pdf>

5.6.2.3 CSP 要員に関するミッションオーナーの責任

上記の要件に加えて、FedRAMP Control Specific Contract Clause v2⁷⁷では、以下のように記載している「FedRAMP 暫定認可を活用している機関は、独自のバックグラウンド調査の実施、またはクラウドサービスプロバイダのシステムを実装した他の機関からの相互主義の受け入れ責任を負う」。また、機関はスクリーニングプロセスに責任を有していて、追加のスクリーニング要件を規定することができる。FedRAMP+アセスメントの一環として、CSP によって使用されるプロセスが評価され、必要に応じて PA の中で議論される。さらに、格付け情報の共有がある時点で必要となり、CSP の職員の中にクリアランスの保持が必要となる場合があるということを、ミッションオーナーに要求される。これは、CSO のユースケースの重要性と情報の重要度またはタイプに基づく。DoD の構成員やミッションオーナーは、すべての職位指定に必要な調査タイプを検討し、調査要件およびクリアランス要件並びに CSP との契約のための資金に対応する必要がある。

5.6.2.4 トレーニング要件

DoD 8570.01-M、「情報保証の要員改善プログラム、更新 3、2012 年 1 月 24 日」⁷⁸は、DoD IA 要員の改善プログラムについて説明している。このマニュアルでは、DoD IA の人員を分類し、経験、訓練、および認定基準を設定している。DoD CSP とミッションオーナーは DoD 8570.01-M に従わなければならない。

影響レベル 6 で運用する CSP は、その職員のために DoD 8570.01-M の要件を満たす必要がある。しかし、影響レベル 2～5 の非 DoD CSP は、これらの要件の範囲外である。しかしながら、すべての影響レベルの CSP は、セキュリティ管理策 AT-3 に記載されているようにセキュリティ要員を訓練する必要がある。商用 CSP で DoD 8570.01-M を課さないという決定は、DoD 以外の顧客にサービスを提供する商用 CSP の人材の雇用および訓練を変更しようとする複雑さに基づいている。商用 CSP セキュリティ要員の訓練は、FedRAMP および DoD PA 評価の一環としてセキュリティ管理策 AT-3 への準拠について評価される。

5.7 データの流出

CNSSI 4009、CNSS 用語集⁷⁹によると、データ流出または「流出」とは、格付けされた情報またはコントロールされた非格付け情報を、データまたは情報の適切なセキュリティレベルで認定されていない情報システムへ許可なく転送することである。

⁷⁷ FedRAMP Control Specific Contract Clauses v2, June 6, 2014;
<https://www.fedramp.gov/resources/documents/>

⁷⁸ DoD 8570.01-M: <http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf>

⁷⁹ CNSSI 4009: <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>

データ流出は、流出の範囲と DoD データへのリスクを最小限に抑えるために、ミッションオーナーと CSP の両方からの即時の報告と対応が必要なサイバーインシデントである。ミッションの所有者は、通常の経路でインシデントの報告を行う。CSP は、セクション 6.5「サイバーインシデントの報告と対応」の要件に従うだけでなく、ミッション／情報所有者に流出を報告しなければならない。ミッションオーナーが自分のデータセット内の流出を検出する可能性は非常に高いが、CSP も流出を検出する可能性がある。CSP による検出は、CSP がミッションオーナーの情報システムのコンテンツに意図的にアクセスする特定のサービス提供に依存している。

クラウド環境は、データ流出の対応に独特な課題を提起している。一般的な IT のデータ流出では、サニタイズによって修復または「クリーン」な状態にして、影響を受けたハードウェアから流出したデータの再構築が不可能または非現実的なことを確実にする。このプロセスでは、物理ストレージメディアにアクセスする必要がある、クリーンアップが完了するまでストレージリソースがオフラインになることがよくある。そのような可用性の喪失は、複数のテナントが同じインフラストラクチャを共有するクラウド環境では受け入れられない。CSP でストレージ仮想化を使用すると、多数の動的なデータインスタンスが生成され、物理的なデータの場所を把握することが困難になる。これにより、物理的なサニタイズ方法は、クラウドサービスにおけるデータ流出修復のために実行不可能になる。これらの課題から、クラウドで発生したデータ流出サイバーインシデントを緩和する方法が必要である。

ミッションオーナーがクラウド環境や IaaS、一部の PaaS CS0 のように、どのようにデータを保存するかコントロールできる場合は、セクション 5.11.1「暗号消去」で説明した暗号消去がそのような方法である。暗号消去は、確実に保存しているデータを読み取ることができないよう保証する高水準の方法である。さらに、ファイルの削除により、ファイルの場所が新しいデータで上書きされる可能性が高くなる。これは通常、使用頻度の高いクラウド環境で頻繁に発生している。CE とファイルの削除は、クラウドサービスで使用する大規模な仮想化環境での物理的なサニタイズよりも迅速かつ実用的である。さらに、暗号鍵を DoD がコントロールすることで、ミッションオーナーは、CSP に不正データの存在を警告することなく、データ流出インシデントに対応することができる。

ただし、CE は暗号化されたデータのオプションに過ぎない。ミッションオーナーは、セクション 5.11「商用クラウドストレージにおけるデータの暗号化・保護」に準拠し、すべての保存データが暗号化されるようにする必要がある。

データ流出を発見した際は、ミッションオーナーは、NIST SP 800-88 Rev 1 に準拠して、関連する解読キーを削除し、不正なデータを暗号消去する必要がある。また、ミッションオーナーは、実行中の VM のメモリの中など、暗号化されていない状態で存在している可能性のある不正なデータの削除など、必要な処置を行う必要がある。

ミッションオーナーや CSP で使用されるデータのバックアップや被害復旧の手段により、データの漏出は関連するストレージにも影響する可能性がある。データ流出の修復は、流出したデータが転送された可能性のある記憶媒体にまで対処が必要である。影響を受けたすべてのバックアップとミラー化されたストレージも、修復する必要がある。ミッションオーナーは、データのすべてのコピーを暗号消去する責任がある。これらの状況下で、流出データの転送を制限するため、適時の検出、報告、および対応が重要である。

CS0 の暗号化されていない状態で不正なデータが格納されていたデータ流出は、そのようなデータを回復不能にするために利用可能なオプションを駆使して、ミッションオーナーが影響の軽減を図る必要がある。このようなインシデントへの対応は、暗号消去よりも確実性の低い方法に限定されるかもしれない。暗号化を利用していない、または使用できないミッションオーナーは、特定の CS0 のすべてのデータ消去オプションを列挙したデータ流出対処手順を作成する必要がある。そのようなインシデントの発見と同時に、許可されていないデータの再構築の危険性を減らすために最高の行動方針を決定するため、リスク分析を実行しなければならない。これは、インシデントの緩和に協力を得るために、認可されていないデータの存在を CSP に警告することを含んでも含まなくてもよい。

ほとんどの SaaS および PaaS CS0 のように、ミッションオーナーがクラウド環境やデータの保存方法を管理していない場合、CSP は、流出が検出されたときにアクティブにできる機能を CS0 内に提供する必要がある。これらの機能は、ミッションオーナーの管理下にある必要がある。暗号化消去に加えて、ファイルまたはデータベースのレコード／フィールドレベルでの細かい DAR 暗号化とデータ削除機能は、そのような機能の一部でなければならない。

CSP は、上記の暫定認可パッケージの一部として、すべての CS0 の能力に関するミッションオーナーの統制に対処する流出是正計画を提出しなければならない。

クラウドデータ流出防止／修復のための代替の革新的な方法は、標準的な方法と同等であるかどうか評価され、十分であると認められる場合には承認される。

対応するセキュリティ管理策：IR-9、MP-6

5.8 CSO から移行のためのデータ処理と破壊

オフ・ボーディングは、ミッションオーナーが CSO の使用を終了したときに行われる一連の活動である。ミッションオーナーが新しいクラウドサービスに移行したり、任務が終了したり、契約が終了したり、CSP が業務を中断したりすると、オフ・ボードプロセスが必要になる。オフ・ボーディング・プロセスは、データ検索／移行とデータのサニタイズまたは破壊という 2 つの段階に分割される。ミッションオーナーは、最終的な CSO オフ・ボーディングに備えなければならない。CSP はその機能をタイムリーにサポートしなければならない。

ミッションオーナーからの要請により、CSP は CSP に保管されているすべてのミッションオーナーのデータを、独自仕様でない標準フォーマットで CSP 環境から電子的に転送することができる。CSP は、ミッションオーナーの CSO 使用に関するすべての監査ログを利用できるようにする必要がある。これには、AU-11 で指定された期間、AU-2 セキュリティ管理策で指定されたすべての監査内容が含まれる。詳細は、セクション 5.2.3 「DoD データの所有権と CSP による DoD データの C 使用」を参照。ミッションオーナーの要求に応じてデータをダウンロードし、データの削除または削除要求を行う CSO は、この要件を満たすための特定の CSP アクションを必要としない場合がある。各ミッションオーナーは、その裁量で、異なるデータ転送手段（たとえば、SLA で呼び出されたもの）を要求することもできる。

セクション 5.11.1 「暗号消去」で説明されている暗号の消去は、保管されたデータの読出しが不可能となることを確実に保証する方法を提供している。CSO からデータが正常に転送されると、残りの暗号化されたデータを持つミッションオーナーは、暗号化されたミッション・データをすべて消去し、暗号化されていない状態で CSO にデータが残らないようにする必要がある。ミッションオーナーが撤収する CSO のインフラストラクチャで維持されているすべてのバックアップも暗号で消去する必要がある。また、ミッションオーナーは、通常の CSP 手順に従って、撤収する顧客に対して、すべてのミッション・データを削除するか、論理的にアクセス不可能にするように要求する必要がある。データのミッションオーナー移転が成功したことを確認した後で、CSP はすぐに削除しなければならない。そうでなければ、ミッションオーナーのデータがすべて回復不可能になる。セクション 5.9 「保管媒体及びハードウェアの再利用と廃棄」に記載されているオフボードが完了した後であっても、ハードウェアの使用終了時に DoD データを保持していたすべてのストレージデバイスのサニタイズまたは破壊は CSP の責任である。

DoD のミッションオーナーは、DoD 以外のサービスを使用している場合、いつでもデータを移行できる必要がある。つまり、ミッションオーナーは、クラウドサービスからのデータを短期間で受け取ることができなければならない。この機能は、利用可能なローカルストレ

ージインフラストラクチャ、または短期間でデータを受け入れることができる別の CSP によって提供されるクラウドサービスの形でサポートできる。これは、ミッションオーナーが CSO の突然の停止時に迅速にデータを取得できるようにするためである。(例えば、CSP が倒産を宣言し、サービスを停止する場合)。この問題は、セクション 5.12 「バックアップ」で説明するように、ミッションオーナーが効果的なバックアップ手順を利用することによっても緩和できる。

対応セキュリティ管理策：DM-2、MP-6

5.9 記憶媒体及びハードウェアの再利用と破棄

CSP は、FedRAMP で選択されたセキュリティ管理策 MP-6 の要求にしたがって、DoD のデータが破棄されて処分された記憶デバイスに残存しないこと、CSP と DoD の間の合意のない環境で再利用されないこと、または第 3 者へ移転されないことを確実化しなければならない。

影響レベル 4/5：CSP は、すべての DoD データが正常に削除されるまで、ストレージハードウェアを再利用または廃棄することはできない。CSP は、NIST SP 800-88、Rev 1 「メディアサニタイズのガイドライン」⁸⁰に従い、破棄、処分、再利用、または移転する前に、最低限デバイス上のすべてのデータを確実に「ページ」する。クリアまたはページできないデバイスは、NIST SP 800-88 Rev 1 で定義されているように物理的に破壊されている必要がある。クリアまたはページされたプロセスが成功するかどうか疑問がある場合は、NIST SP 800-88 Rev 1 に従ってストレージデバイスを破壊する必要がある。

影響レベル 6：オンプレミス CSP はストレージハードウェアを低いセンシティブリティまたは格付けレベルで処分したり再利用したりすることはできないが、格付けされたデータは NSA/CSS Storage Device Declassification Manual 9-12 に従ってサニタイズすることによって破棄されたデバイスからの回復を不可能とする⁸¹。

対応セキュリティ管理策：DM-2、MP-6

⁸⁰ NIST SP 800-88:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

⁸¹ NSA/CSS 9-12:

https://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf

5.10 アーキテクチャ

CC SRG のこのセクションでは、DoD が利用する DoD および商用クラウドサービスの次の分野での利用に関連するさまざまなアーキテクチャ上の考慮事項について説明している。

- CSP のインフラストラクチャ／ネットワークと DISN 間の接続
- CSP サービスの保護と必要な DoDIN サイバー空間防衛およびアクセス制御サービスへの統合
- ミッションシステム／アプリケーションの保護と必要な DoDIN サイバー空間防衛とアクセスコントロールサービスの統合

DoD の商用クラウドサービスの利用は、DoD がインターネットに接続された CSP/CSO のエコシステムに加わることを意味している。DoD はインターネットに接続された CSO を公開情報の配布または処理（レベル 2）に活用しているが、DoD は同じ CSO へのプライベート接続で、センシティブな DoD 情報（レベル 4 および 5 の CUI）の保護に活用している。さらに、NIPRNet にネイティブではない DoD ミッションパートナーは、レベル 4/5 処理（おそらく免除の下で）にインターネット接続された CSO を活用する必要がある、または独自のプライベート接続を実装する必要がある。

図 10 の NIPRNet／商用／連邦クラウドエコシステムは、NIPRNet が接続されているオフプレミス、Non-DoD プライベート-商用および連邦 CSP/CSO で構成されるクラウドエコシステムの全体的なアーキテクチャを示している。図中の CSP/CSO クラウドのいずれかは、商用 CSO または非 DoD 連邦機関が運用／提供する CSO であってもよい。この図の要点は、CSO にレベル 4/5 の PA があり、プライベート接続を介して NIPRNet に接続されている場合でも、すべての非 DoD プライベート商用や連邦 CSP/CSO がインターネットからアクセス可能であることをはっきりと確認できることにある。また、これらの CSP/CSO が非 DoD 顧客をサポートしていることも示している。この図は、大半のミッションユースケースの商用／連邦 CSO への NIPRNet 接続に焦点を当てている。すべての可能な状況や使用例を示しているわけではない。追加の図が CC SRG の将来のリリースで提供されるかもしれない。

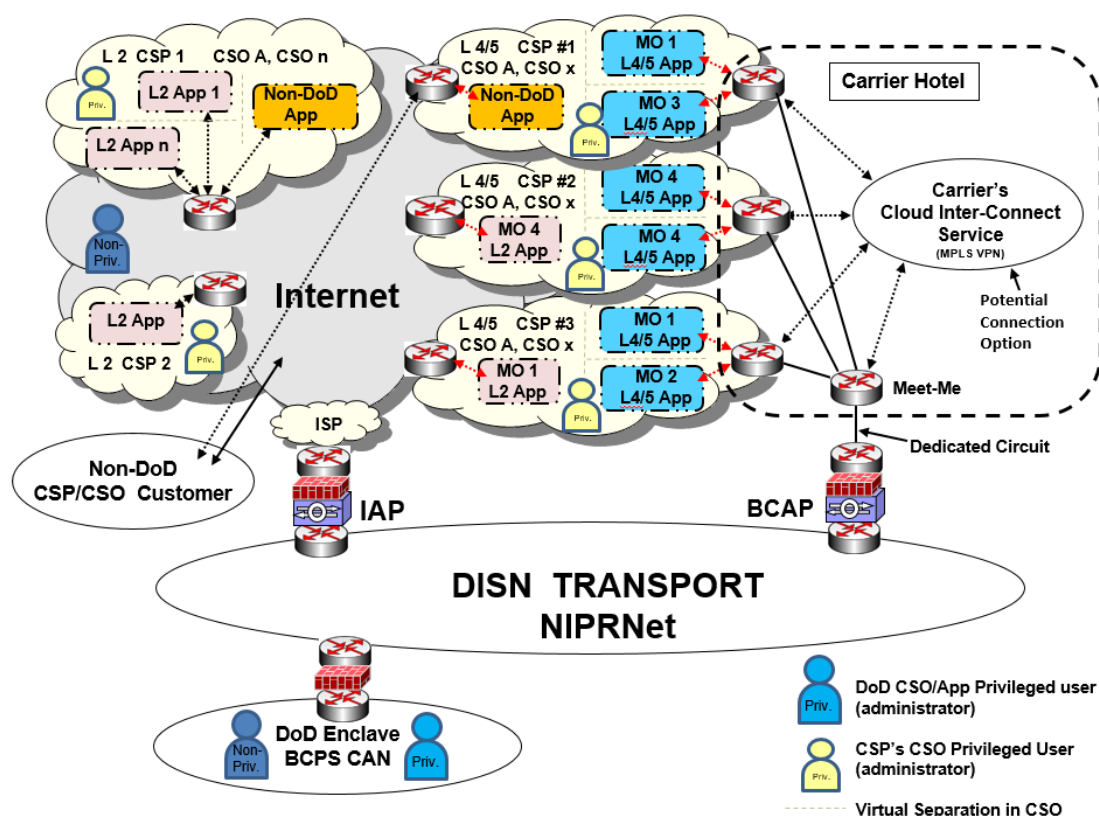


図 10 NIPRNet/商用/連邦クラウドエコシステム

5.10.1 クラウドアクセスポイント (CAP: Cloud Access Point)

クラウドアクセスポイント (CAP) の概念と要件は、DoD CIO の「DoD Cloud Way Forward、v1, 2014 年 7 月 23 日」⁸²に記載されている NSA および DoD サイバーセキュリティチームのガイダンスに基づき、CSO が所有し商用で運用しているオフプレミスおよびオンプレミスに対しセキュリティスタック/CAP を提供するものである。このコンセプトは、2014 年 12 月 15 日の DoD CIO メモで、「商用クラウド・コンピューティング・サービスの取得および利用に関するガイダンスの更新」で方針を示したもので、「センシティブなデータ用の商用クラウドサービスは、クラウドアクセスポイント (CAP) を通じて顧客に接続する必要がある」と述べている。この CC SRG は概念を拡張し、オンプレミスとオフプレミスの CSO に対する要件の微調整を行う。

この SRG の目的上、DoD CIO メモで参照されるセンシティブなデータは、レベル 4/5 で扱われる CUI、またはレベル 6 で扱われる SECRET までの機密情報を意味している。

⁸² DoD Cloud Way Forward: http://iase.disa.mil/Documents/dodciomemo_w-attachment_cloudwayforwardreport-20141106.pdf

一般に、一定の制限下を除き、商用 CSO を接続することによってもたらされる DISN（または他の DoD ネットワーク）へのリスクを軽減するには、CAP が必要である。CAP は、ネットワークの境界保護および監視デバイス（ファイアウォール、IPS、IDS、プロキシなど）のシステムで、サイバーセキュリティまたは IA スタックとも呼ばれ、CSP インフラストラクチャとネットワークと CAP の保護するネットワークを接続する。この CC SRG は、DISN を保護されたネットワークとして扱っているが、これには NIPRNet、SIPRNet、または他の DISN ベースのミッションパートナー/COI (Community of Interest) ネットワークを含む。

CAP の主な目的は、CSP のインフラストラクチャ、CSO 管理プレーン、CSP の企業ネットワーク、CSP のインターネットへの接続、侵害されたミッションオーナーのシステム/アプリケーションと仮想ネットワークから発せられた無許可のトラフィックからの DISN（または他のネットワーク）の保護と検出である。2 次的な目的は、ネットワークユーザが IaaS/PaaS でインスタンス化されたレベル 4/5 または 6 のミッションオーナーシステム/アプリケーションにアクセスするための保護された接続を容易にし、または SaaS を使用し、トラフィックをインターネットにさらすことなく情報の保存・処理を行うことによって DoDIN（すなわち DoD 情報）を保護することにある。これらの目的は、ネットワークを保護するためのミッションパートナーまたは COI ネットワーク上のすべての CAP およびそれらに含まれるセンシティブな情報にも適用される。

注意：CAP は、アプリケーションまたはアプリケーションが存在するネットワークエンクレーブ（物理または仮想）を保護するものではない。I/PaaS のアプリケーションの仮想環境に組み込まれているものを管理する各ミッションオーナーは、アプリケーションと仮想ネットワークの保護区域を保護する必要がある。ミッションオーナーが P/IaaS アプリケーションの環境に組み込まれているものを制御できない P/SaaS などの CSO の場合、CSP がアプリケーションの保護と、アプリケーションが存在するネットワークエンクレーブ（物理または仮想）に責任を持つ。

CAP アーキテクチャは、CSO インフラストラクチャがオンプレミスかオフプレミスか、そしてサービスがそれを通過するかどうかによって変化する。オンプレミス CSO の内部 CAP（ICAP: Internal CAP）の概念と、オフプレミス CSO の境界 CAP（BCAP: Boundary CAP）の概念について、DISN を保護するためのこれらの実装方法に焦点を当て、以下で詳しく説明する。一部の CAP は既存のインフラストラクチャを活用し、一部は新しい機能である。CAP アーキテクチャは DoDIN ネットワーク、または保護している COI ネットワークに応じて変化する。

DoDIN サイバー防衛をサポートするために提供しなければならない CAP の基本的な機能は以下のとおりである。

- CSO から特定の DISN DoD エンドポイントへ特別に許可されたトラフィックを除き、CSO とその管理プレーンを発信元とするすべてのトラフィックを拒否し、CSO へのアウトバウンド（DISN からの）要求に対するインバウンド（DISN への）応答のみを許可するファイアウォール機能（すべて許可）。これにより、CSO 管理プレーンまたは侵害された CSO からの不正な DoDIN/DISN アクセスの可能性が取り除かれる。
- 暗号化されていないトラフィックで伝達されたファイアウォール障害、不正なトラフィック、マルウェアやその他の悪意のあるトラフィックを検出する IDS（Intrusion Detection）機能
- SIP-TLS および SRTP プロトコル（または許可されていない非セキュアバージョン）で構成される Voice over IP（VVoIP）トラフィックが CAP を通過する場合、SBC（Session Border Controller）機能を実装する必要がある。SBC 機能は、back-to-back SIP ユーザエージェント／プロキシモードで実装する必要があるため、TCP/UDP ポートは静的にインバウンドシグナリングで開かれない。SBC 機能は、メディア（SRTP）用のランダムに選択されたエフェメラル UDP ポートを動的に管理して、これらの IP ポートが通信セッションの期間だけ開かれるようにする必要がある。さらに、SBC 機能は、不正な活動、誤った／欠落したパケットなどを検出し報告する SIP/SRTP IDS として動作する必要がある。

注：上記のすべての機能は、DoDIN 境界サイバー防衛機能に情報を流して異常を検出し、ネットワークおよび IS 上の他の異常と関連させる必要がある。

このセクションの残りの部分では、DISN 接続 CSO の CAP 要件を定義している。これらの概念は、DISN Transport を使用せず、DISN IAP の背後にない他のネットワークにも適用できる。

対応するセキュリティ管理策：SC-7、SC-7（3）、SC-7（4）

5.10.1.1 境界 CAP（BCAP）

オフプレミスで CSO が所有し運用している DISN（または他のネットワーク）に接続するには、境界 CAP（BCAP）が必要である。BCAP は、プライベート接続サービスを提供する複数の CSP ネットワークで保護するネットワークの相互接続を行う。BCAP は、CSP CSO、その上に構築されたミッション・アプリケーション、またはネットワークユーザとの間で直接のインターネットアクセスを提供しない。

一般に、BCAP は次の保護を提供している：

- CSO でホストされているアプリケーションとの間のトラフィックに対し、DISN 境界防衛とサイバー防衛検知を提供
- 特定の CSP のインフラストラクチャまたはサポートされているミッションに影響を与えるインシデントから、DISN およびそのネットワークサービスと共に DoDIN (つまり、DoD 内の DoD ミッションと情報) の保護
- ある CSP のインフラストラクチャでインスタンス化された DoD のシステム/アプリケーションを、異なる CSP のインフラストラクチャまたはサポートされるミッションに影響を及ぼすインシデントからの保護

DISN BCAP は、エンクレーブ及び DISN とその他、相互接続された情報システムを保護するための DISN 境界である。DISN は境界の内側または保護された側に位置する。同様に、I/PaaS または P/SaaS で実装されたミッションオーナーのシステム/アプリケーションは、エンクレーブ境界と DMZ 保護を必要とするエンクレーブと見なされる。これらは境界の外側または保護されていない側に位置している。I/PaaS や P/SaaS アプリケーションに実装されているミッションオーナーのシステム/アプリケーションは、それ自体を保護する必要がある。これは可能な限りアプリケーションエンクレーブの境界線の近くで達成する必要がある。ミッションオーナーが VM および環境を制御できる IaaS および PaaS に実装された複数のミッションオーナーのシステム/アプリケーションは、仮想データセンターセキュリティスタック (VDSS: Virtual Datacenter Security Stack) によって保護され、セキュア・クラウドコンピューティングアーキテクチャ (SCCA: Secure Cloud Computing Architecture) 機能要件文書 (FRD)⁸³ (現在ドラフト中) で説明されている仮想データセンター管理スイート (VDMS: Virtual Datacenter Management Suite) を通して管理される。ミッションオーナーが PaaS または SaaS を使用する場合、ミッションオーナーは VM および環境を管理できないので、CSP が CSO に与えた保護に頼るか、代替ソリューションサービス (たとえば最低限、FedRAMP Moderate PA を持つクラウドアクセスセキュリティブローカー (CASB: Cloud Access Security Broker) を活用する。

5.10.1.1.1 NIPRNet BCAP

NIPRNet の DISN BCAP 機能の実装は、DoDIN と DoD の情報を保護するというミッションの一環として、最終的には DISA 責任である。2014 年 12 月 15 日の DoD CIO メモでは、DoD CIO の承認を得て、DISA 以外の DoD コンポーネントによって一時的に機能が提供される場合が

⁸³ SCCA FRD: http://iase.disa.mil/cloud_security/Pages/index.aspx (PKI required)

あるものの、DISA がエンタープライズ全体の DISN サービスとして DISA BCAP を実装することを目指している。この要件は、ICAP ではなく NIPRNet への境界 CAP に適用される。特定の CAP アーキテクチャの要件は、この SRG の範囲を超えており、SCCA FR ドキュメントで個別に公開される。

NIPRNet BCAP は、超冗長、デュアルホーム、地理的な分散、高可用性、大容量のサイバーセキュリティスタックと meet-me ポイントとしてのシステムとして実装されなければならないため、BCAP システムは商用クラウドへ移行予定のすべてのアプリケーションを処理するために必要なスループットを処理できなければならない。これは、DISN ユーザと複数のオフプレミスのレベル 4/5 CSO との間の接続を提供する。また、これらの CSO へのインターネットからのインターネット接続サービス (IFA) 用の DISN インターネットアクセスポイント (IAP) を通じたユーザ接続を容易にしている。

影響レベル 2：レベル 2 PA を持つオフプレミスの CSP インフラストラクチャは、インターネットに直接接続され、レベル 2 の CSO レベル 2 ミッションとそのミッション仮想ネットワークとの間のすべてのトラフィックは、インターネットを経由することから、NIPRNet BCAP は使用されない。NIPRNet のユーザは、これらの CSO とアプリケーションを DISN インターネットアクセスポイント (IAP: Internet Access Points) 経由でアクセスするが、インターネットベースのユーザは直接アクセスを行う。I/PaaS CSO に実装されたミッションオーナーアプリケーションは、独自のエンクレーブ境界と DMZ アプリケーション保護を提供するか、同じ CSO 内でインスタンス化されたエンタープライズレベルのアプリケーション保護サービス (つまり、SCCA の仮想データセンターセキュリティスタック (VDSS: Virtual Datacenter Security Stack) / 仮想データセンター管理スイート (VDMS: Virtual Datacenter Management Suite)) を活用しなければならない。VDSS/VDMS は、DISA、DoD コンポーネント、またはミッションオーナーによって提供されることがある。SaaS CSO は、ミッションオーナーが追加の保護サービス (CASB など) を利用する独自のエンクレーブ境界と DMZ アプリケーション保護を提供する必要がある。詳細については、5.10.2.2「ユーザ／データプレーンの接続性」、および 5.10.2.3「管理プレーンの接続性」を参照のこと。あるいは、レベル 2 の IFA をレベル 4/5 の CSO に実装し、NIPRNet BCAP を介して接続を行う。下記の影響レベル 4/5 を参照。

注：公開された情報へのアクセスを提供するすべての IFA と、機密性の低い個人情報へのアクセスを提供する一部の IFA は、レベル 4 または 5 の CSO ではなく、レベル 2 の CSO に移行する必要がある。これにより、BCAP インフラストラクチャの負荷と必要容量が削減されるだけでなく、DoD のコンポーネントと部門が最大のコスト削減を実現し、その他の必須とされるコスト削減イニシアチブをサポートできるようになる。

影響レベル 4/5 : NIPRNet（または他の COI ネットワーク）と、レベル 4 およびレベル 5 のミッションを提供する CSP インフラストラクチャやミッション仮想ネットワーク間のすべての DoD トラフィックは、1 つまたは複数の NIPRNet BCAP を通過する必要がある。ミッションオーナー、DoD コンポーネント、または DISA によって提供される NIPRNet IAP および DoD DMZ 機能を経由しない限り、インターネットへの直接トラフィックは許可されない。BCAP または接続された meet-me ポイントは、CSN がアクセスされる DISN と CSP のネットワークとの間の直接的な物理的または論理的接続を提供する。物理的な接続性は、DISN meet-me ポイントルータと近くの CSP ネットワークルータとの間の直接光ファイバ接続を使用して確立される。論理接続は、専用長距離回線、プライベート IP VPN サービス、FedRAMP 認定マルチ CSP/顧客相互接続サービス、またはポイントツーポイント IPsec VPN を使用して確立される。これらの接続は、CSP のネットワークインフラストラクチャやミッションオーナーの仮想ネットワーク内で発生する IPsec VPN 接続の転送をサポートすることもできる。これには、非特権ユーザアクセスの運用プレーンと特権ユーザアクセスの管理プレーンが含まれ、内部 DISN ネイティブ・サイバーセキュリティ防衛監視システムへの IA/サイバーセキュリティ防衛ツール接続が配備されている。詳細については、セクション 5.10.2.2 「ユーザ/データプレーンの接続性」と 5.10.2.3 「管理プレーンの接続性」を参照のこと。高可用性ミッションオーナーシステムとそれをサポートする CSP ネットワークインフラストラクチャは、2 つ以上の NIPRNet BCAP を介して接続する必要がある。

NIPRNet BCAP は、次の機能も提供している。

- レベル 4 の CSO が提供している IFA やミッションシステムに対する認定された DoD の DMZ として機能し、ミッションシステム/アプリケーションで使われる DoD の IP アドレスに面した DISN が DoD の認定 DMZ IP を提供する。ミッションオーナーのアプリケーションは、独自の DMZ アプリケーション保護を提供するか、DISA またはクラウドの DoD コンポーネントによって提供されるエンタープライズレベルのアプリケーション保護サービス（SCCA の仮想データセンターセキュリティスタック（VDSS）/仮想データセンター管理スイート（VDC））を活用する必要がある。BCAP は、レベル 4/5 CSO への直接インターネットアクセスをサポート/提供していない。そのようなアクセスは、NIPRNet IAP を経由しなければならない。
- DoD コンポーネントの DMZ 拡張の内部側からの物理接続または論理接続を終了させて、DoD コンポーネントの既存の DMZ/DMZ 拡張保護を IFA 用に利用することができる。

注意 : レベル 5 の CSP/CSO インフラストラクチャ/アプリケーションと DoD ミッションオーナーアプリケーションは、インターネットベースのリソースに依存しないように設計されていなければならない。したがって、BCAP を介して接続された CSO および DoD ミッショ

ンオーナーアプリケーションは、DoD がインターネットへの NIPRNet アクセスを遮断することを決定した場合でも、NIPRNet に接続しているユーザにサービスを提供する機能を完全に提供することができなければならない。もちろん、このような状況では、インターネット接続されたユーザはレベル 5 のサービス／リソースを利用することができない。レベル 4 の CS0 に対してこの制限が必要なミッションオーナーは、SLA／契約に要件を追加する必要がある。

5.10.1.1.2 NIPRNet BCAP Meet-Me ポイント

NIPRNet BCAP Meet-Me Point は、キャリアに依存しない商用ネットワーク相互接続設備または商用通信事業者のコロケーション設備に位置する DISN 接続点 (PoP : Point-of-Presence) である。この PoP は、最小限の容量のルータで構成されるが、BCAP サイバーセキュリティスタックの全部または一部を構成する DISN 境界保護機能を含む場合がある。

BCAP Meet-Me Point の目的は、DISN BCAP と複数の CSP ネットワークとの相互接続を容易にすることである。複数の BCAP Meet-Me Point の実装により、CSP ネットワークとの相互接続による冗長で信頼性の高い接続を実現している。BCAP Meet-Me Point は、接続の可用性を向上させ、ユーザと CS0 の間のレイテンシーを短縮するために、米国の管轄区域内で地理的に分散されている。BCAP や Meet-Me ポイントは、複数の CSP ネットワーク (例えば、Equinix Cloud Exchange、AT&T NetBond、および Verizon Secure Cloud Interconnect) へのクラウドカスタマーネットワークアクセス／接続を提供する商用キャリアグレードサービスとの相互接続をサポートすることもできる。

Meet-Me Point は商用施設にある DISN PoP であるため、次の要件が適用される。商用施設に位置する BCAP Meet-Me Point/DISN PoP の要件

- ケージなどの商用施設内の物理的に隔離された保護されたスペースに設置するか、最低限でもロックされたキャビネットにする必要がある。物理的に離れたスペースは、最低限でも以下の保護が必要とされる。
 - 商業施設への物理的なアクセスは FedRAMP の中位または高ベースライン (PE と MA ファミリ) の必要なすべての物理的環境および保守要員のアクセスセキュリティ管理策に準拠するとともに、ロールベースのアクセス制御、アクセスの監査、ロギング及び必要に応じたエスコートなどが必要である。
 - DoD スペースへの物理的アクセスは、FedRAMP の中位ベースラインまたは高ベースラインや CNSSI 1253 ベースラインのすべての必要な物理的および保守要員のアクセスセキュリティ管理策に準拠するとともに、ロールベースのアクセス制御、アクセス監査、必要に応じて訪問者のエスコートなどが必要である。
 - DoD スペースへの要員のアクセスは、トークンやバイオメトリックベースの自動エントリーアクセス制御システム (AECS:Automated Entry Access Control

System) によって制御される。このシステムは、DoD の管理下にあるか、施設所有者の管理下にあるかもしれないが、許可された人だけにアクセスを制限し、アクセスおよび退去する人物のアイデンティティを含むすべてのアクセスを記録／監査し、無許可のアクセスや失敗した試行に関するログやアラートを提供しなければならない。

- 。 物理スペースへのアクセスは、ビデオカメラと物理的侵入検知システム (IDS) アラームシステムを使用して施設の所有者によって外部から監視される。

- 。 DoD により運用される自動モーション IDS システムとビデオカメラで内部スペースを監視することを強く推奨。これにより DoD は、許可／不許可にかかわらずスペース内のすべての身体活動を監視することができる。

- DoD SRG および STIG に準拠しなければならない。
- 承認された接続とシステム修正のすべての模様を文書化する変更管理および接続承認プロセスに従わなければならない。
- すべての接続に対し、追跡および認可の目的でコマンド通信サービス指定子 (CCSD: Command Communications Service Designator) が割り当てられる。

DISN 認可の境界の延長としての役割のために、BCAP および DISN 認定の一環として DoD RMF の下で評価され、認可されなければならない。

5.10.1.1.3 BCAP 接続のための CSP サポート

DoD とオフプレミスでレベル 4/5 CSP 間の BCAP 接続をサポートするには、CSP はインターネットを経由しない CSO にプライベート接続サービスを提供する必要がある。CSP のネットワークには、既存の DISN PoP/BCAP Meet-Me-Point が配置されているキャリアに依存しない商用ネットワーク相互接続設備または商用通信事業者のコロケーション設備に PoP を含める必要がある。施設内の物理的な接続は、2 つの PoP の間に設置され、DISN BCAP と CSP のネットワークとの間に直接的なプライベート接続を提供し、CSO はサポートサービスと共にアクセスされる。信頼性が CSO へのアクセスの要件である場合、相互接続は、少なくとも地理的に分散された 2 つのネットワーク相互接続／コロケーション設備においてに実装されなければならない。

DoD レベル 4 またはレベル 5 の PA の条件として、CSP は CSO へのアクセスのためのプライベート接続サービスを提供する必要がある。DoD は、CSP に 1 つまたは複数の PoP が DISN BCAP の Meet-Me-Point と連携していない可能性があることを認識している。このような CSP ネットワークが存在する中で、PA 取得については PoP を必要としないが、そのような PoP のインストールまたは相互に合意可能な DISN と CSP PoP の隣接した場所についての調整、

または適切な仲介クラウド相互接続サービスの利用（DoD 用の PA を持つ）を行う。関連コストは、ミッションオーナーと CSP の間で交渉される。新しい DISN Meet-Me PoP が必要な場合、その交渉に DISA を含める必要がある。この潜在的な状況の通知は、PA 評価フェーズ中に提供する必要がある。かかる交渉は、CSP とその最初のミッションオーナーとの間の契約に基づく BCAP 接続の計画段階で行われる。また、ミッションオーナーは、CSP が 1 つまたは複数の DISN meet-me-point と一緒に PoP を持っていなければならないことを規定している。

5.10.1.1.4 インターネットと BCAP への CSP / CSO ネットワーク接続性

セクション 5.10 「アーキテクチャ」と図 10 「NIPRNet/商用/連邦クラウドエコシステム」は、NIPRNet BCAP を介して NIPRNet に接続されたレベル 4/5 PA を持つ CSP/CSO もインターネットに接続されているという現実を示している。

DoD レベル 4 またはレベル 5 PA のための条件として、DoD 契約 CSO をサポートする CSP のネットワークが、NIPRNet BCAP（または BCAP を介して他の DoD ネットワーク）およびインターネットを介して NIPRNet ヘブライベートに接続されている場合、CSP のネットワークまたは CSO がインターネットから NIPRNet（または他のネットワーク）へのパスを提供して、DoD ネットワークへのバックドアとはならない証拠を提示しなければならない。追加的または関連する考慮事項は、インターネットベースの脅威からの保護のために、インターネットと CSO との間に実装された CSP の必要な境界保護（多層防護/防護措置）の堅牢性である。この防護は、CSO が I/PaaS であるか P/SaaS であるか、およびミッションオーナーが CSO の一部を支配するかどうかによって異なると予想される。詳細は、5.10.3 「CSP サービスアーキテクチャ」および 5.10.6 「IaaS/PaaS を利用したミッションオーナーのシステム/アプリケーションの要件」を参照。

5.10.1.2 内部 CAP (ICAP)

ICAP は、DISN（またはその他のネットワーク）または CSO が接続されているデータセンタネットワーク（境界内/保護された側）を CSP のインフラストラクチャ（境界の外部/非保護側）、外部接続された CSO 管理プレーン、CSP 企業ネットワーク、インターネットへの CSP 接続、および侵害されたミッションオーナーシステム/アプリケーションおよび仮想ネットワークから保護するサイバーセキュリティスタックで構成された DISN 境界である。通常、1 つの ICAP インフラストラクチャインスタンスごとに 1 つの ICAP が必要である。

影響レベル 2/4/5 : CSO 管理プレーンがネイティブ NIPRNet エンクレーブおよび外部境界保護をバイパスする外部ネットワークへの接続性を備えている場合、オンプレミスで商用として所有され、運用されている DISN への CSO 接続用に内部 CAP (ICAP) が実装される。

そのため、レベル 2、4、5 のミッションとミッション仮想ネットワークにサービスを提供する、オンプレミスで商用の CSP インフラストラクチャとの間で行われる NIPRNet（または他の格付けなしの COI ネットワーク）のトラフィックは、ICAP を通過する必要がある。

ICAP には、オンプレミス（例えば、B/C/P/S 内の物理的または仮想的な「フェンスライン」内）の商用 CSP の CSO インフラの実装に伴う脆弱性とリスクの低減が求められる（そのインフラが CSP の社内ネットワークやインターネットと何らかの接続を持つ可能性が高い、DoD 管理外のワークステーションやインフラを使った CSO 管理センターから、オフプレミスの CSP によって管理される場合）。CSO 管理センターとオンプレミス CSO の管理プレーンとの間の接続は、NIPRNet、その IAP、およびインターネットを介した IPSEC トンネル、または専用線によるサイドドア、商用通信事業者のプライベート IP VPN サービス、または制限されたインターネットサービスプロバイダ（ISP）接続を想定している。CSP が VPN を必要とする ISP 接続では、CSO 管理プレーンとの間でインバウンドまたはアウトバウンドアクセスを提供してはならない。この要件は、CSO 管理プレーンが CSO にローカル専用であり、オンプレミスで管理されていても、CSP の企業ネットワークなどへの外部接続がある場合にも適用される。

ICAP は、CSO を使用するミッション・アプリケーションに対して、承認された運用トラフィック（すなわち、承認された IP ポート上に必要なプロトコルおよびサービス）を通過するように設定され、CSO 管理プレーンから、CSO が接続されている DISN またはデータセンターネットワークへのすべてのアクセスをブロックする。

ICAP のアーキテクチャは、BCPS 上の CSO インフラストラクチャの位置、既存のインフラストラクチャ、およびその他の要因に基づいて変更され、開発される。ICAP は、最低限ファイアウォール機能と IDS 機能で構成されているが、DoD データセンター（現在）（すなわち DECC）、JIE コアデータセンター（CDC）（将来）などを保護するサイバーセキュリティスタックや、ジョイント・リージョナル・セキュリティ・スタック（JRSS: Joint Regional Security Stack）などの既存機能を利用できる。一方、ICAP には、特定のミッション、CSP タイプ（商用または DoD）、または特定のクラウドサービスをサポートするための特別な機能を有する場合がある。CSP インフラストラクチャと ICAP はどちらも NIPRNet に直接接続されているか、DoD データセンターネットワーク経由で間接的に接続されているため、BCAP 境界保護のフル装備は不要である。

今日の DoD データセンター（DECC など）または JIE コアデータセンター（CDC）を ICAP として保護するサイバーセキュリティスタックを使用する場合、CSN は DISN とデータセンターネットワークの両方が CSO 管理平面から保護されるように接続する必要がある。

ICAP の実装とオンプレミス CSP インフラストラクチャの NIPRNet への接続は、DoD データセンター内の NIPRNet エンクレープまたはアプリケーションインフラストラクチャの場合と同様に、通常の NIPRNet 接続承認ガイダンスと要件に従う。

CSO が以下の条件の下で管理されている場合、ICAP は必要とされない。

- CSO 管理プレーンが、非 DISN ネットワークへのサイドドアまたはバックドア接続を持たない CSO インフラストラクチャの一部であるクローズドネットワークまたは
- CSO 管理プレーンが、ネイティブの NIPRNet 境界保護および IAP を介して、インターネットまたは CSP 企業ネットワークなどの外部ネットワークとのみ接続可能な NIPRNet エンクレープまたはその一部。CSP の要員は、ワークステーションから社内ネットワークに VPN 接続することができるが、CSP のネットワークと CSO 管理プレーンの間でポイントツーポイント VPN が確立されないことがある。后者では ICAP の設立を要求される。

さらに：

- CSP 要員が、DoD 設置/BCPS の場所から CSO を管理
- CSP 要員のワークステーションが CSO の管理業務を遂行するに際し NIPRNet にアクセスできる場合 GFE が提供される。
- CSP 要員は、CSO の管理の一般的なビジネス機能を実行するために必要とされる電子メールやインターネットサーフィンなどに、同じ GFE を使用することはできない。
- CSP 要員は、設置/BCPS アクセスおよび GFE や NIPRNet へのアクセスのための CAC カードが発行される。

5.10.1.3 SIPRNet BCAP/ICAP

国家シークレットファブリックのための CNSS のアーキテクチャ推奨に従って、DoD SECRET エンクレープおよび DoD のオンプレミスの影響レベル 6 の CSO でインスタンス化された仮想ネットワークは、DoD プロバイダネットワーク (SIPRNet) 内のエンクレープとみなされる。

管理ネットワークを含めるために DoD のオン/オフプレミスの影響レベル 6 の CSO とそのサポートインフラストラクチャは、1 つ以上の閉じた SIPRNet エンクレープである必要があるため、この CC SRG の目的の上、そのような DoD エンクレープの周りに仮想「フェンスライン」または SIPRNet 境界を拡張するという考え方により、オンプレミスにあると考える

ことができる。したがって、これらのエンクレーブは、適切なエンクレーブ境界保護とサイバー空間防衛の要件を含む SIPRNet 接続承認要件すべてに準拠する必要がある。これらの影響レベル 6 の CSO エンクレーブでインスタンス化された DoD ミッションオーナーのシステム/アプリケーションは、他の DoD SIPRNet エンクレーブ接続と同じ方法で評価され、承認される。

したがって、これらの DoD エンクレーブ（物理または仮想）を SIPRNet に接続するには、SIPRNet BCAP は必要とされない。

さらに、レベル 6 のミッションおよびミッション仮想ネットワークにサービスを提供するオンプレミス、業者所有で CSP により運用されるインフラストラクチャと SIPRNet（またはその他の格付け COI ネットワーク）とのトラフィックは、CSO がオフサイトで管理されている場合（一般的ではない）にのみ ICAP を通過する必要がある。ICAP は、CSO を使用しているミッション・アプリケーションに対して許可された運用ラフィックを通過させ、CSO 管理プレーンから接続されている DISN またはデータセンターネットワークへのすべてのアクセスをブロックする。オンプレミス CSO がオンプレミナ場所から管理されている場合には、CSO と管理場所が 1 つまたは複数の SIPRNet エンクレーブとみなされ、そのように保護されるため、この場合は適用されない。

5.10.1.4 ミッションパートナーの環境またはコミュニティネットワークのクラウドアクセスポイント

この CC SRG の目的上、ミッションパートナーは DoD のコンポーネント、連邦機関、DoD およびその他の組織を含むネットワークを運用する請負業者を指す。このセクションでは、戦闘連合国のパートナー、または彼らが使用している、またはそれらのために実施されているネットワークは含まない。連合ネットワークは、CC SRG の将来のリリースで対処されるかもしれないが、これらのネットワークでのクラウドコンピューティングの利用は、この SRG がネットワークの格付けレベルに応じて NIPRNet または SIPRNet へ BCAP と ICAP を含めるのと同じ方法で実装されるべきである。

ミッションパートナー環境（MPE:Mission Partner Environments）には、NIPRNet や SIPRNet（DREN など）以外のネットワークや NIPRNet や SIPRNet（例えば、MilCOI）を活用するネットワークオーバーレイやエクステンションを利用するミッションパートナーコミュニティ（COI）などのミッションパートナーが含まれる。さらに、DoD のミッションパートナー（カミサリー、エクステンジ、モラル・福祉・レクリエーション（MWR）機関、厚生資金組織（NAF:Non-Appropriated Fund）、国防防衛大学（NDU））などは通常、DISN や .mil ドメインの一部ではない（NIPRNet IAP 経由のインターネットアクセスなどの DISN トラン

サポートまたは NIPRNet サービスを使わない)。これらのミッションパートナーとそのネットワークは、.gov/.org/.com/.edu ドメインであり、それらが運用し承認した、または契約した第3者の DHS/GSA トラステッド・インターネット接続 (TIC:Trusted Internet Connection) により、DoD の IAP と同様の境界を介してインターネットから直接アクセスすることができる。そのような、他のネットワークと COI は、NIPRNet または SIPRNet と相互接続され、他の DoD および非 DoD ミッションパートナー/機関ネットワークと相互接続することができる。

ここに提示されている CAP の概念は、他の DoD コンポーネント (例えば、様々な非 DoD ユーザーベースをサポートする .edu コミュニティ) によって運営されているネイティブ DISN ネットワーク以外にも適用可能であるが、商用クラウドを利用することに伴うリスクからネットワークを保護するための手段は、他にも存在している。最低限 FedRAMP 中位の PA を有するクラウドアクセスセキュリティブローカー (CASB : Cloud Access Security Broker) サービスが、DISN 以外のネットワークの代替手段の一候補となる可能性がある。

NIPRNet や SIPRNet (例えば DRSN) 以外のネットワークを利用する MPE は、CSP インフラストラクチャをネットワークに接続する際に、SCCA 機能要件文書 (FRD) ⁸⁴で定義されたものと同等の保護を提供するネットワークに対して BCAP または ICAP を実装する必要がある。NIPRNet または SIPRNet に COI オーバーレイとして実装された MPE は、DISA が提供する CAP を使用して CAP 要件を満たすことができ、SCCA に基づいて独自の CAP 機能を提供できる。しかし、NIPRNet または SIPRNet の外部のミッションパートナーは、DoD データと MPE を外部サービスプロバイダへの接続に関連する脆弱性から保護する同等の機能を提供する責任がある。

すべての MPE CAP インスタンス化は、DoD CIO の承認を得なければならない。

注：このような CSO でインスタンス化された MPE アプリケーションに接続/アクセスする場合、オフィスで商用、DoD レベル 4/5 CSO への MPE ネットワーク接続/アクセスは、NIPRNet BCAP または NIPRNet フェデレーテッド・ゲートウェイ (NFG:NIPRNet Federated Gateway) を通過しない。

5.10.1.5 クラウドでホストされている NIPRNet サービスへアクセスするミッションパートナーの環境

NIPRNet サービスへのアクセスを必要とするミッションパートナーの環境は、インターネット経由、IAP 及び DoD DMZ、または JFHQ-DODIN TASKORD 16-0103 に従って NIPRNet フェ

⁸⁴ SCCA FRD: Link to be added when published

デレーテッド・ゲートウェイ (NFG) 経由で NIPRNet へ接続する必要がある。NIPRNet サービスは、NIPRNet ユーザにサービスを提供する目的で DoD コンポーネントによって運用されるアプリケーションである。これらの NIPRNet に焦点を絞ったアプリケーションの一部は、CSO で実装される可能性がある。そのような CSO は、商用のオンプレミス CSO、DoD のプライベートオンプレミス CSO、または DoD のプライベートオンプレミス CSO である。そのようなアプリケーションへのアクセスを望んでいるまたは必要としているミッションパートナーは、そのアプリケーションへのアクセス許可を得て最良のアクセス方法を決定するために、アプリケーションのミッションオーナーと調整する必要がある。そのようなアプリケーションにアクセスするには、次の 3 つの承認された方法がある。

- MPE ユーザは、NIPRNet またはアプリケーション自体に VPN 接続を確立する必要がある。
- ミッションオーナーは、MPE ユーザが IAP を介してインターネットからアプリケーションにアクセスできるように、DoD DMZ を介してアプリケーションをインターネットに公開する必要がある。
- ミッションオーナーは、NFG を通じて MPE ネットワークと MPE ユーザへアプリケーションを公開する必要がある。

5.10.1.6 DISN BCAP を介したミッションシステムの接続承認

影響レベル 4/5 : ICAP または BCAP を介して DISN のミッションシステムへの接続は、通常の接続承認手順に従って DISA 接続承認オフィスによって承認され記録される。これにより、すべてのミッションオーナーは、すべてのクラウドベースのアプリケーション、CSP/CSO、および接続方法を DISA システム/ネットワーク承認プロセス (SNAP:Systems/Network Approval Process) ⁸⁵データベースのクラウドモジュールに登録する必要がある。CSP の最初のミッションオーナーの顧客のオンボード中に、CSP のネットワークへの初期接続 (物理または仮想) が発生する。ある CSP を、より多くのミッションオーナーが使用するにつれて、追加の接続が行われるか、容量が拡大される。BCAP を介した接続承認およびミッションオーナー接続に関する特定のプロセスおよび手順は、最終的に全体の DISN 接続プロセスガイド (CPG:Connection Process Guide) ⁸⁶とマージされる DISA クラウド接続プロセスガイド (CCPG) ⁸⁷で対処されている。

⁸⁵ SNAP: <https://snap.dod.mil/gcap/home.do>

Connection Approval: <http://www.disa.mil/Network-Services/Enterprise-Connections/Connection-Approval>

⁸⁶ CPG: http://disa.mil/~media/Files/DISA/Services/DISN-Connect/References/DISN_CPG.pdf

⁸⁷ CCPG: <http://disa.mil/~media/Files/DISA/Services/DISN-Connect/References/CCPG.pdf>

影響レベル 6：影響レベル 6 の CSO エンクレーブでインスタンス化された DoD ミッションオーナーのシステム／アプリケーションは、DISA CPG による他の DoD SIPRNet エンクレーブ接続と同じ方法で評価され、承認される。SIPRNet への接続の承認は、他の SIPRNet エンクレーブと同様、DISA に基づく接続承認プロセスを通じて処理される。

5.10.2 ネットワークプレーン

ネットワーク・コンテキストでは、ネットワーク・アーキテクチャの 3 つの不可欠なコンポーネントの中の 1 つである。データ同期／制御またはネットワークプレーン、ユーザ／データまたは運用プレーン、および管理プレーンの 3 つの要素は、異なる操作領域と考えることができる。各プレーンは異なるタイプのトラフィックを運び、概念的にはネットワークプレーンの上にあるオーバーレイネットワークである。

5.10.2.1 ネットワークプレーンの接続性

ネットワークまたはデータ同期／制御プレーンは、シグナリングトラフィックおよびサーバー／データセンター間のデータの複製を運ぶ。ネットワーク制御パケットは、ネットワーク転送装置（仮想または物理）から発信されるか、またはその宛て先である。一般に、ネットワークプレーンは、ネットワーク関連の DoD SRG および STIG の影響を受ける。この CC SRG には、クラウドコンピューティングインフラストラクチャへのネットワークプレーン接続に関連する追加の要件は含まれていない。

5.10.2.2 ユーザ／データプレーンの接続性

ユーザ／データプレーン（転送プレーン、キャリアプレーン、またはベアラプレーンとも呼ばれる）は、ネットワークユーザトラフィックを伝送する。表 5 は、DoD オンプレミスおよびオフプレミス CSO の影響レベル別の DoD ユーザ／データプレーンの接続性を示している。

注：この表は、DoD のオンプレミス CSO を使用している非 DoD の政府機関のテナントには適用されるが、DoD テナントを持つ連邦政府のコミュニティクラウドであるオンプレミス CSO を使用した非 DoD の連邦政府テナントには適用されない。

表 5 ユーザ／データプレーンの接続性

影響レベル	オフプレミスで Non-DoD の CSP によるサービス提供のインフラ	オンプレミスで DoD 及び Non-DoD の CSP によるサービス提供のインフラ
-------	--------------------------------------	---

<p>レ ベ ル 2</p>	<ul style="list-style-type: none"> ・ユーザの接続は、商用インフラストラクチャ（インターネットなど）を活用する。 ・インターネットから接続しているユーザは、DISN 内（つまり、NIPRNet）から接続しているユーザが DISN インターネットアクセスポイント（IAP）経由でインターネットに接続し、次に CSP インフラストラクチャに接続する。 ・CSO 接続は、他のインターネット接続と同じ外部接続要件を適用して評価され、許可される。 	<ul style="list-style-type: none"> ・ユーザ接続は、ユーザが B/P/C/S フェンスライン（オンプレミ）内にあり、ローカルベースエリアネットワーク（BAN: Base Area Network）および NIPRNet に直接接続されている場合、そのユーザ／データプレーンに対して既存のインフラストラクチャ（政府所有）を使用する。 ・NIPRNet と CSO インフラストラクチャ間のユーザトラフィックは、ICAP を通過する。ユーザがインターネットに接続された B/P/C/S フェンスライン（オフプレミス）外にある場合、ユーザトラフィックは、DISN インターネットアクセスポイント（IAP）を経由して NIPRNet に入り、DoD の DMZ を経由して ICAP へ入出する必要がある。
<p>レ ベ ル 4 及 び 5</p>	<ul style="list-style-type: none"> ・DoD および外部ユーザ接続は、政府境界内の政府ネットワークインフラストラクチャ（すなわち、NIPRNet）および政府境界を越える商用インフラストラクチャ（すなわち、商用キャリアインフラストラクチャ／接続サービスの提供者）を使用して商用施設への DISN 拡張を活用する。 ・DISN 拡張は BCAP を通過する。 ・DISN（すなわち、NIPRNet）の内部から接続するユーザは BCAP を介して接続し、一方、インターネットから接続するユーザは IAP を通過し、その後、DoD DMZ エクステンションを介して BCAP を通過する。 ・CSO 接続は、他の DoD またはイ 	<ul style="list-style-type: none"> ・CSO 接続は、他の内部接続と同じように評価され、承認される。

	<p>ンターネット接続と同じ要件を使用する他の内部接続と同様に、接続承認プロセスを通じて評価され、承認される。DMZ STIG⁸⁸に従って、インターネットに接続された接続が評価され、許可される。</p>	
レベル 6	<ul style="list-style-type: none"> ・ユーザ接続は、政府の境界（すなわち SIPRNet）内の政府 SECRET ネットワークインフラストラクチャおよび政府境界を越える商用インフラストラクチャ（すなわち、商用通信事業者インフラストラクチャ／接続サービスの提供物）を使用して商用施設への DISN 拡張を活用する。 ・商用施設への DISN のエクステンションは、マルチプロトコルラベル ス イ ッ チ ン グ （ MPLS: Multiprotocol Label Switching）ルータおよび光スイッチ（サービスデリバリノードと呼ばれる）を利用して実行できる。 ・商用施設への DISN エクステンションは、NSA タイプ 1 暗号化または商用の同等品（商用ソリューション分類プログラム（CSfC: Commercial Solutions for Classified Programs）⁸⁹スイート B）を使用する。 	<ul style="list-style-type: none"> ・ユーザ接続は、そのユーザ／データプレーン（すなわち SIPRNet）に対して既存の SECRET ネットワークインフラストラクチャ（政府所有）を使用する。 ・SIPRNet へのユーザトラフィックは、ICAP を通過する。インターネットへのユーザトラフィック（例：エグゼクティブトラベルキットユーザ）は、NSA Type 1 暗号化または商用ライセンス（CSfC Suite B）を使用し、承認済みゲートウェイ経由で SIPRNet に入出する必要がある。 ・CSO 接続は、他の SIPRNet 接続と同じ要件（つまり、DMZ STIG に従う）で、他の内部接続と同じように評価され、承認される。

⁸⁸ DoD DMZ STIG:

https://powhatan.iiee.disa.mil/stigs/downloads/zip/fouo_dod_internet-niprnet_dmz_technology_v3r3_stig.zip (CAC/PKI required)

⁸⁹ Commercial Solutions for Classified Programs:

https://www.nsa.gov/ia/programs/csfc_program/index.shtml

	<ul style="list-style-type: none">・インターネットへのユーザトラフィック（例：エグゼクティブトラベルキットユーザ）は、NSA Type 1 暗号化または商用ライセンス（CSfC Suite B）を使用し、承認済みゲートウェイ経由で SIPRNet に入出する必要がある。	
--	--	--

5.10.2.3 管理プレーンの接続性

管理プレーンでは、ネットワーク／サーバー／システム特権ユーザ（管理者）トラフィックと、保守および監視トラフィックが通過する。

表 6 は、ミッションオーナーのシステム／アプリケーションおよび CSP CSO の影響レベル別の管理プレーンの接続性を示している。ミッションオーナー管理プレーンには、IaaS/PaaS 上でインスタンス化されたミッションオーナーシステム（すなわち、仮想マシンおよびネットワーク）を管理する DoD 要員または DoD の請負業者、ならびに DoD 要員または DoD 請負業者のための接続が含まれており、CSP サービス発注／管理ポータルすべてのサービス提供タイプ（IaaS/PaaS/SaaS）の場合 CSP 管理プレーンには、CSP のサービス提供インフラストラクチャを管理する CSP 担当者のための接続が含まれている。

特に明記されていない限り、識別されたすべての暗号化は、FIPS モードで動作する FIPS 140-2 検証済み暗号化モジュールを使用して実行する必要がある。

ベストプラクティスとセキュリティ要件に従って、ミッションオーナーの仮想ネットワークに位置する仮想マシンや保護対象のアプライアンスの管理インターフェースは、運用ネットワーク（例えばインターネットや NIPRNet/SIPRNet）からの直接的なアクセスにさらしてはならない。可能な限り、VM や仮想ネットワークをインスタンス化して構成する CSP サービス発注／管理ポータルも、ミッションシステムと DoD 情報の侵害を防ぐために、運用ネットワークからの直接アクセスから保護する必要がある。

すべての管理トランザクションを監査する必要がある。

表 6 ミッションオーナーの管理プレーンの接続性

影響レベル	ミッションオーナーの管理プレーン	CSP の管理プレーン
-------	------------------	-------------

レベル 2	<p>・ NIPRNet の外部からの管理接続（例えば、オフプレミスの請負業者の要員）は、インターネットを介してミッションシステム／アプリケーションおよび仮想ネットワークへの暗号化トンネル接続を必要とする。CSP サービス発注／サービス管理ポータルへの管理トラフィックは、暗号化された VPN でなければ暗号化する必要がある。監視トラフィックは、VPN 接続を通過する必要がある。NIPRNet に出入りするすべてのトラフィックは、DISN インターネットアクセスポイント（IAP）経由でなければならない。</p> <p>・ NIPRNet 内部からの管理接続（例えば、オンプレミスの DoD または請負業者の要員）によるアプリケーションと仮想ネットワークの管理は、定義された IP アドレスのセットに制限されていなければならない。IAP を介して NIPRNet を介してインターネットへの暗号化トンネリング接続が必要である。暗号化された VPN 外の場合は、CSP サービス発注/サービス管理ポータルへの管理トラフィックを暗号化する必要がある。監視トラフィックは、VPN 接続を通過する必要がある。すべてのトラフィックは、DISN インターネットアクセスポイント（IAP）経由で NIPRNet に出入りする必要がある。</p>	<p>・ インフラストラクチャとオフプレミスの管理を提供する非 DoD CSP オフプレミスサービス:CSP 管理接続は、論理的または物理的にプロダクションとは別の CSP サービス提供および管理プレーンインフラストラクチャを活用する。注: DoD は、DoD 専用ではない商用サービスを CSP がどのように設計するか指示することはできない。DoD は、よく知られている業界のベストプラクティスとして、運用と管理プレーンを提供するサービスの論理的または物理的な分離を推奨している。そのような分離は、DoD のリスク受入れのための要点として評価される。</p> <p>・ インフラストラクチャと管理を提供する非 DoD CSP オンプレミスサービス:CSP は、隣接している場合、管理インフラストラクチャをサービス提供インフラストラクチャに直接接続する場合がある。CSP のオンプレミス管理インフラストラクチャから、サービスプロバイダのオンプレミスサービス提供インフラストラクチャへの暗号化されたトンネリング接続も、ローカルで許可され、リモートサービス提供インフラストラクチャにアクセスするために使用する必要がある。</p> <p>・ 非 DoD CSP オンプレミスサービスのインフラストラクチャおよび</p>
レベル 4 及び 5	<p>・ NIPRNet 内部からの管理接続は、定義された IP アドレスのセットに限定されていなければならない。ミッションシステム／アプリケーションと仮想ネットワークを管理するために NIPRNet と ICAP または BCAP を介した暗号化トンネリング接続が必要である。CSP サービス発注</p>	

	<p>／サービス管理ポータルへの管理トラフィックは、暗号化された VPN でなければ暗号化する必要がある。監視トラフィックは、VPN 接続を通過する必要がある。すべてのトラフィックは、BCAP 経由で NIPRNet に入出する必要がある。</p> <p>・ NIPRNet 外からの DoD 要員または DoD 請負業者による管理接続は、定義された IP アドレスのセットに制限されていなければならない。ミッションシステム／アプリケーションおよび仮想ネットワークへの IAP および ICAP または BCAP を介したインターネットからの暗号化トンネリング接続が必要である。リモート管理ポリシーにより、リモート管理端末は官給品 (GFE: Government Furnished Equipment) でなければならない。暗号化された VPN 外の場合は、CSP サービス発注／サービス管理ポータルへの管理トラフィックを暗号化する必要がある。監視のトラフィックは、BCAP と NIPRNet 経由で VPN 接続とする必要がある。</p>	<p>オフプレミス管理: CSP 管理接続は、CSP のオンプレミス管理インフラストラクチャからサービスプロバイダのオンプレミスサービス提供インフラストラクチャへの暗号化トンネル接続を活用する必要がある。</p> <p>・ DoD CSP のオンプレミスサービスでインフラストラクチャと管理の提供: CSP 管理接続は、エンタープライズサービス部門 (ESD Enterprise Services Directorate:) アウトオブバンド (OOB: Out of Band) 管理ネットワークなどの既存のインフラストラクチャを活用する。サービスプロバイダのセキュリティスタックは必要とされない。</p>
レベル 6	<p>・すべての管理およびモニタリング接続は SIPRNet を介して行われる。管理と監視トラフィックは、Need-to-Know の理由からの分離に対応するため、FIPS 140-2 で検証された暗号⁹⁰により暗号化される。</p>	<p>・ DoD CSP オンプレミスサービスによるインフラストラクチャと管理: CSP 管理接続は、SECRET アウトオブバンド (OOB: Out of Band) 管理ネットワークなどの既存の SECRET ネットワークインフラストラクチャを利用しする。サービスプロバイダのセキュリティスタックは必要とされない。</p> <p>・ 非 DoD CSP オンプレミスサービス</p>

⁹⁰ FIPS 140-2 validated cryptography:
<http://csrc.nist.gov/groups/STM/cmvp/index.html>

		<p>ス提供とインフラストラクチャと管理：CSP の要員が SECRET LAN を使って隣接している場合、管理インフラストラクチャをサービス提供インフラストラクチャに直接接続する場合があります。CSP のオンプレミス管理インフラストラクチャからサービスプロバイダのオンプレミスサービス提供インフラストラクチャへの SIPRNet を介した FIPS 140-2 検証済み暗号化を使用する暗号化されたトンネリング接続も許可され、リモートサービス提供インフラストラクチャへのアクセスに使用される。</p> <p>・ 非 DoD CS オンプレミスサービスの提供とオフプレミス管理：CSP の管理接続は、CSP の専用 SECRET オフサイト管理インフラストラクチャからサービスプロバイダのオンプレミスサービスへの SIPRNet 拡張機能または DoD で承認された暗号化されたトンネリング接続を利用する必要がある。</p> <p>・ 非 DoD CSP オフプレミスのサービス提供インフラストラクチャとオフプレミス管理：CSP 管理接続は、論理的または物理的に分離された CSP の専用の SECRET サービスと管理プレーンインフラストラクチャを利用する。</p>
--	--	---

5.10.3 CSP サービスアーキテクチャ

DoD は、ネットワークとデータ／情報を保護する際に、縦深防御という概念を使用している。これには、ホスト OS とアプリケーションの堅牢化、ホストファイアウォールと侵入検知の実装、強力なアクセス制御、イベントの強力な監査、アプリケーション層のファイアウォール、プロキシ、Web コンテンツフィルタ、電子メールゲートウェイ、侵入検知／防止、DMZ／ゲートウェイアーキテクチャと同時に堅牢なネットワークトラフィック監視機能を備えている。ミッションオーナーのシステム／アプリケーションとそのデータ／情報を商用クラウドに移行する際に、その概念を失ってはならない。したがって、仮想化を使用する場合は、ハイパーバイザベースのファイアウォール／フィルタリング／ルーティングメカニズムまたは仮想セキュリティアプライアンスの使用とともに、仮想環境を保護するために上記の対策も活用する必要がある。

このセクションでは、DoD のデータ／情報およびミッションシステム／アプリケーションを保護するために、CSP およびミッションオーナーが実装する必要のある縦深防御のセキュリティの概念と要件について詳しく説明している。DoD は、物理ネットワークとサーバーで長年培ってきた縦深防御策のいくつかを置き換える可能性がある、仮想環境に実装できる革新的なアプローチがあることを認識している。DoD は、ケースバイケースで DISA によって評価される同等の代替措置を評価することを楽しみにしている。

5.10.3.1 CSP サービスアーキテクチャ - SaaS

CSP の SaaS サービスを利用しているミッションオーナーは、CSP がサービスアプリケーションの保護とそれをサポートするインフラストラクチャの保護のために実装した縦深防御策に依存している。これには、CSP インフラストラクチャに格納され、処理されるすべての機密情報の保護が含まれる。言い換えれば、ミッションオーナーは、DoD 情報の保護のために CSP と SaaS 提供のセキュリティの体制に依存している。SaaS 提供についての AT0 アセスメントプロセスの間に、縦深防御セキュリティ／保護処置の適切性と DoD の潜在的リスク受理に向けて評価されなければならない。これは、セキュリティ管理策の評価に加えて行うことができる。以下のガイダンスは他のオペレーティングシステム (OS) と特定用途向け STIG とともに DoD DMZ STIG とアプリケーションセキュリティと開発 STIG で反映されるが、信頼すべき引用 (例えば、製品に特有の STIG) が利用できない例を強調するために、ここで取り上げている。

SaaS を対象として CSP によって構築される縦深防御セキュリティ／保護処置は、次のとおりであるが、これに限定されるものではない。

- アプリケーション層のファイアウォール (適切に構成された)、侵入検知／防止による

SaaS アプリケーションをサポートする CSP のインフラ保護、と同様に CSP の他の製品や企業ネットワークからの（論理または物理的な）セグメンテーション化。

- アプリケーション／データベースサーバーおよびその他のサポートシステム／サーバーの適切な保護を備えたプライベート／バックエンドゾーンやインターネット／外部に面したサーバーについて、DoD DMZ STIG に従って適切に保護された制限なし／制限ありの DMZ ゾーンを提供するアプリケーション／ネットワークのアーキテクチャ。これには、保存／処理されるアプリケーションや顧客のデータ／情報の保護に必要とされる、Web アプリケーションファイアウォール、リバース Web プロキシ、FTP プロキシなどを含むが、これらに限定されるものではない。
- FIPS 140-2 で検証され FIPS モードで動作する暗号化モジュールを使用した、ミッションオーナーのみがキーを制御できる、顧客の保存データの暗号化保護。この要件は、顧客のデータをさまざまなメディアやデータベースに永続的に保存する場合に適用され、顧客のデータの保存なしでリアルタイム処理を要求する場合には適用されない。そのようなデータが保持されていれば、保持されたデータ記憶は永続的である。
- FIPS 140-2 で検証された FIPS モードで動作する暗号化モジュールを使用した顧客のデータ転送中の暗号化保護。この要件は、パブリックおよびプライベート（WAN）（すなわち、インターネット、NIPRNet、CSP の WAN）およびローカルエリアネットワーク（LAN）を顧客端末から CSP のサービス提供エンクレーブ LAN に転送する顧客データに対応する。暗号化は、プロトコルレベルでネイティブでも、VPN／トンネルレベルでもかまわない。この要件は、プライマリロケーションとバックアップ運用継続性（COOP：Continuity of Operations）／被害復旧（DR:Disaster Recovery）ロケーション間の顧客データおよびシステムの CSP レプリケーションにも適用される。
- 業界標準に準拠した OS およびアプリケーションの堅牢化／パッチ適用／保守。サービスが DoD で使用されているプライベートクラウドまたはコミュニティクラウドの場合は、DoD SRG と STIG または DoD で受け入れられた同等のサービスを使用する必要がある。情報保証（IA:Information Assurance）脆弱性管理（IAVM:IA Vulnerability Management）メッセージに準拠するため、CSO は DoD IAVM メッセージで参照される CVE で特定されたパッチを適用することで、業界のベストプラクティスに準拠することが期待されている。すべてのシステムに対して挙動ベースまたはソフトウェアの完全性保護モデルを実装するなどの革新的な代替案は実行可能であり、ケースバイケースで評価される。
- 影響レベル 4 および 5 の情報を IA-2（12）に従って処理する SaaS 製品におけるすべてのカスタマーユーザアクセスに対する PIV/DoD CAC/PKI 認証の実装。これには、サービスへアクセスする正規の非特権ユーザとサービス注文／管理インターフェース／ポータルにアクセスする特権の顧客ユーザが含まれる。影響レベル 6 で情報を処理する SaaS 製品は、CNSS SIPRNet トークンを使用する必要がある。必要な PKI トークンを使用で

きないユーザコミュニティの代替認証手段は、ケースバイケースで評価され、免除が必要な場合がある。

注：DoD SRG および STIGS で提供される脆弱性緩和と同等のものが実行可能で容認可能であるが、DISA AO の承認を得なければならない。

注：IAVM メッセージには IA 脆弱性警告 (IAVA: IA Vulnerability Alerts)、IA 脆弱性速報 (IAVB: IA Vulnerability Bulletins)、および技術勧告 (TA: Technical Advisories) が含まれている。この SRG の残りの部分では、IAVM という用語はすべての IAVM メッセージタイプを参照するために使用される。

5.10.3.2 CSP サービスアーキテクチャ - IaaS/PaaS

ミッションオーナーは、IaaS/PaaS の下で CSO が提供する仮想インフラストラクチャ上にシステムとアプリケーションを構築する。CSP とミッションオーナーとの間のセキュリティに対する責任の明確な記述がなければならない。これは、CSP が CSO でサポートするセキュリティ機能をどのように提示するかによって異なる。IaaS のもとでは、ミッションオーナーは、ゲスト OS とゲストアプリケーションのセキュリティを完全に担う責任がある。CSP は、仮想化 OS (すなわち、ハイパーバイザ) を保護し、インフラストラクチャをサポートする責任を負う。PaaS のもとでは、ミッションオーナーは、ゲストオペレーティングシステムと、プラットフォームアプリケーションとアプリケーションのセキュリティを完全に担う責任がある。CSP CSO が CSO でサポートするセキュリティ機能をどのように提供するかに応じて、ゲストオペレーティングシステムおよびプラットフォームアプリケーションに関して責任の構図がミッションオーナーから CSP に部分的に移行することがある。CSP は、コアサービスの一部として、またはアドオンコンポーネントとして、PaaS CSO のこれらの領域を保護する責任を負う可能性がある。

この SRG の残りの第 5 章の目的では、IaaS および PaaS の提供は、一般に、ミッションオーナーのものである OS およびプラットフォームアプリケーションを保護する責任と同様に扱われる。ミッションオーナーは、縦深防護／防護要件が完全に満たされているかどうかを判断するために CSP が提供する継承された緩和を評価する必要がある。

CSP の IaaS および PaaS 製品は、ミッションオーナーがその上に構築するシステムおよびアプリケーションを保護するために実装を求められている縦深防護セキュリティ／防御対策をサポートする必要がある。これらの措置はセクション 5.10.6「IaaS/PaaS を利用したミッションオーナーのシステム／アプリケーションの要件」で定義されている。

5.10.3.3 CSP 被害復旧 (DR) - 運用の継続性 (COOP)

ビジネス上のベストプラクティスとして、CSP は被害復旧 (DR: Disaster Recovery) と運用の継続性 (COOP: Continuity of Operations) を計画し、そのインフラストラクチャを実装してサポートを行う。これには通常、地理的に離れた施設／データセンターが含まれる。さらに、FedRAMP は、緊急時対応計画（すなわち、DR および COOP）に関連するいくつかの C/CE の評価を行う。

バックアップを含む被害復旧 (DR) や運用の継続性 (COOP) のため、地理的に離れた施設／データセンター間でのデータ複製が通常必要である。

すべての複製データは、CSP 提供のサイト／ロケーションから DR/COOP 施設への CSP のプライベート内部ネットワーク（物理または仮想）を通過させて、転送中のデータを保護する必要がある。このネットワークがインターネットを通過する場合、FIPS 140-2 で検証された暗号化を使用して実装された IPsec トンネルで、ネットワーク接続をエンドツーエンドで暗号化する必要がある。CSO 提供サイト／ロケーションで DoD データと非 DoD データの間で CSO に実装されている分離要件は、DR/COOP 施設で複製する必要がある。そのような分離は、終点施設での分離をサポートするためにその実施が要求されない限り、転送中には特に必要とされない。

注：レベル 4/5 CSO の場合、DR/COOP 施設がオンプレミスであるか、別の CSP の CSO でない限り、このような転送は DISN BCAP を経由しない。

関連コントロール：CP-6、CP-7、CP-9

5.10.4 インターネットプロトコル(IP)のアドレス指定とドメインネームサービス(DNS)

DoDI 8410.01 「インターネットドメイン名の使用および承認、2015 年 12 月 4 日」⁹¹は、DoD 組織、その IS およびネットワークによるトップレベルドメイン (TLD: Top Level Domain) 名の使用に関する DoD ポリシーを提供している。

DoDI 8410.01 は、DoD の .mil TLD のために設立された TLD のもとで、DoD に公開および民間のインターネットベースの通信（電子メールや Web 操作など）を行うことを DoD に要求している。必要に応じて、.gov、.edu、および .com ドメインを使用する可能性があり、ミッションオーナーの CIO によって承認される一部の DoD の組織には例外がある。つまり、URL を使用して DoD Web サイトや他のリソースにアクセスするエンドユーザは、URL の最後に「.mil」と表示される（たとえば、name.com ではなく、name.mil）。

⁹¹ DoDI 8410.01: <http://www.dtic.mil/whs/directives/corres/pdf/841001p.pdf>

DoDI 8410.01 では、さらに DoD が ARIN(American Registry for Internet Numbers)によって DoD に割り当てまたは指定された IP アドレスのドメイン名として .mil のみを使用し、これらの IP が DoD の NIC レジストリプロトコル 9802 に従って指定されることを要求している。DoD NIC レジストリプロトコル 9802 は、次のように規定している。

- a. IP アドレス空間は、DoD の共通ユーザデータネットワーク上での使用のために DoD の NIC によって割り当てられ、商用インターネットサービスプロバイダを介したインターネットへのアクセスを得るために使用することはできない。

そして

- b. IP アドレス空間は、それが登録されている共通のユーザネットワーク上でのみ使用される。IP アドレス空間または IP アドレス空間のサブネットは、異なる共通ユーザネットワーク間で共有されることはない。たとえば、SIPRNET で使用する IP アドレス空間は SIPRNET でのみ使用する必要があり、NIPRNET で使用する IP アドレス空間は NIPRNET でのみ使用する必要がある。

これを解釈すると、DoD の IP アドレスは、登録された DoD ネットワーク上にある DoD システムでのみ使用される。

さらに、.mil の URL は、.mil ドメイン外のホスト（たとえば、name.mil は name.com にリダイレクトされない）へリダイレクトされないようにする必要があり、唯一の例外は、承認され、認定されたサービスでエンドユーザには容易には見分けがつかない（例えば、コンテンツ配信サービスまたはクラウドサービスの使用）サービスである。この例外は、商用 IP アドレスに関連付けられた CSP によって割り当てられた URL に URL をリダイレクトする DoD DNS サーバー内のシステムの DNS レコードに標準名（CNAME:Canonical Name）を使用することを可能にする。そのように、エンドユーザに対して、リダイレクトを容易に意識させてはならない。

注：DoDI 8410.01 パラグラフ 3.a の電子メール（email）とこのセクションの前の例は、サービスにアクセスするための URL が「.mil」で終わることを条件に、DoD コンポーネントによる外部の商用クラウド電子メールサービスの使用を否定するものではなく、またリダイレクションはユーザには明らかではない。

注：ARIN から DoD NIC に割り当てられ、さらに DoD コンポーネントのネットワークおよび情報システム（例えば、NIPRNet アドレス）へ割り当てられる IP アドレスは、パブリッ

クにルーティング可能なユニークなアドレスである。DoD ネットワークエンクレープ内でのみ許可／使用されている（公開ルーティングができない）RFC 1918 のプライベートアドレスである。

5.10.4.1 IP アドレッシング

オフプレミス・影響レベル 2 IaaS/PaaS/SaaS :

オフプレミスで影響レベル 2 の IaaS/PaaS/SaaS CSO はインターネットから直接アクセスされるため、影響レベル 2 の IaaS、PaaS、SaaS の CSO は、CSP によって指定され管理されているパブリック IP アドレスの利用を求められる。これは、.mil ドメイン名以外を利用することを許可された DoD ミッションオーナーのシステム／アプリケーションにも適用される。この場合、DoD の DNS サーバーは .mil URL に CNAME を使って、商用の URL とその IP アドレスを指定する。

注：インターネットに面したインターフェースが、仮想ネットワークエンクレープ内の RFC 1918 「プライベート」 IP アドレスと共に商用のアドレスを使用することは容認されるが、トポロジー隠蔽のために最小限とすることが推奨されている。

オフプレミス・影響レベル 4/5 :

DoD IP アドレスは DoD のネットワークインフォメーションセンター（NIC: Network Information Center）によって割り当て／管理され、さらに DoD コンポーネント NIC によって管理され、ネットワークと IS を割り当てられる。DoD ポリシー NIPRNet に従って、サブネット化されたコンポーネントエンクレープネットワークとその内部接続されたエンドポイントは、DoD の NIPRNet IP アドレスを指定される。

注：以下は、非 DoD、非 NIPRNet、IP アドレスを使用することがすでに承認されていて、NIPRNet に接続されていない、または NIPRNet の一部ではない DoD システムには適用されない。このような DoD システムを NIPRNet の一部にすることを意図していない。

デフォルトでは、IaaS および一部の PaaS CSO でインスタンス化されたミッションオーナーのシステム／アプリケーションは、CSO でインスタンス化されたシステム／アプリケーションの IP アドレッシングを完全に制御できるため、NIPRNet BCAP、DoD NIPRNet IP アドレスが使用される。これは、ミッションオーナーが CSO の部分で使用されている IP アドレッシングを制御できる SaaS にも当てはまる。したがって、これらのシステム／アプリケーションは、NIPRNet の拡張とみなされるネットワークエンクレープ内にある。DoD NIC は、NIPRNet BCAP に接続された CSO のための NIPRNet IP アドレスの範囲を確保している。この要件は、

BCAP が必要な NIPRNet 以外のネットワークにも同様に適用される。そのような場合、当該ネットワーク上でその IP アドレスが使用される。

注：DoD のどのエンクレープの場合と同様に、BCAP を介して接続された NIPRNet／インターネット対向インターフェース上の NIPRNet アドレスを持つ仮想ネットワークエンクレープ内の「プライベート」RFC 1918 IP アドレスの使用は容認される。

DoD NIPRNet IP アドレスをプライベート接続および BCAP を介して利用できるよう、顧客に面したインターフェースについて、CSO が「独自の IP アドレスの持ち込み」を可能とすることが、DoD に提供されているすべてのオフプレミスでレベル 4/5 CSP の CSO のための DoD の方針要件である。この場合、顧客に面したインターフェースには、CSO 顧客サービス管理／発注ポータルを含む一般ユーザインターフェースおよび顧客管理インターフェースを含む。DoD は、CSO の初期セットアップ中を除き、インターネット経由でそのようなポータルへのアクセスを要求されることを望まない。

この IP アドレッシングの要件には、CSO インフラストラクチャ内で、顧客が直面していないか、NIPRNet（または他のミッションパートナーネットワーク）から直接アクセスできない CSP システムは含まれない。そのような内部システムおよびインフラストラクチャは、CSP によって割り当てられ管理された IP アドレスを使用することができる。

レベル 4/5 商用 IP アドレス指定とルーティング：

DoD は、現在、オフプレミスの商用 SaaS および PaaS CSO の一部では、「独自の IP アドレスを持っている」場合と同様に CSO の IP アドレッシングを制御できないため、CSP は商用 BCAP 経由で IP アドレスを使用し、NIPRNet と接続する必要があることを認識している。DoD の優先ソリューションは、CSP が CSO と NIPRNet BCAP の間に NAT またはプロキシを提供して、NIPRNet が DoD IP アドレスだけのルーティングで済ませることである。

免除：CSO の商用 IP アドレスを NIPRNet 上でルーティングする必要がある代替ソリューションは、CSO が DoD PA を授与される能力に影響を与える可能性があり、非 DoD アドレッシングのリスクアセスメントおよび免除プロセスによって評価および承認されなければならない。DoD PA は条件付となるかもしれない。CSP は、DISN/NIPRNet の運用とサイバーセキュリティの影響を最小限に抑えるため、このような代替ソリューションを実現するには DISA と協調して調整する必要がある。

以下は、非 DoD アドレッシング免除／PA 条件について検討される最小限の制約と要件のセットであり、進行中の運用のために守らなければならない事項である。

- ベンダーは、そのようなルーティングを行うために、NIPRNet でルーティングする必要のある商用 IP サブネットの完全なリストを提供するものとする。
 - これらのルート広告は、現在の DISN 機能をサポートするために/24 以上のブロックに集約する必要がある。時間の経過と共に変化が予想されるが、DISA オペレーターの管理負担を軽減し、ネットワークサービスの中断を減らすために、リストの変更の頻度は最小限に抑えなければならない。
- オフプレミスの CSO の DoD サービスとアプリケーションにアクセスするために使用される BCAP 経由で NIPRNet に広告された商用 IP サブネットは、CSP のインフラストラクチャからインターネットに広告してはならず、もしそうであればインターネットから到達できてはならない。言い換えれば DoD ポリシーに従って、NIPRNet だけからアクセスできる L4/5 DoD アカウント、サービス、およびアプリケーションは、インターネットから直接アクセスできないようにする必要がある。
- DoD は、CSO の L4/5 DoD アカウント、サービス、およびアプリケーションにアクセスするために使用される CSO の商用 IP アドレスが、BCD およびプライベート接続を介して DoD アクセス専用になることを期待している。ただし、CSD/CSO のすべての顧客 (DoD または非 DoD) のアクセスに CSO が同じ IP アドレスを使用する必要がある場合 (これは非 DoD 顧客のアクセスがインターネット経由であることを前提としている)、CSO のインターネット接続や侵害されたシステムが NIPRNet のバックドアになるのを防ぐため、CSP は特別な注意を払わなければならない。
- DISA は、CSP の商用 IP サブネットを NIPRNet IAP 経由でインターネットに広告しない。広告すると、インターネットからの CSO への不正なトラフィックが NIPRNet を通過しようとする可能性がある。DISA は、運用上およびサイバーセキュリティ上の理由から、このようなトラフィックをサポートすることはできない。.mil URL に関連付けられた DoD IP アドレスのみが、IAP を介してインターネットに広告される可能性がある。
- ミッションオーナーが、他のミッションオーナーによっても使用されている CSO の BCAP とイントラネットゲートウェイ/境界間に「クラウド」VPN を実装している場合、同じ商用 IP アドレスが NIPRNet、インターネット、ミッションオーナーのイントラネットからも見えて到達できるかもしれない。この場合、ミッションオーナーは、独自のルーティングポリシーを管理する責任がある。ミッションオーナーは、通常のシナリオと障害シナリオの両方で、サービスのアクセス制御を実施するために、ネットワーク内にルーティングとセキュリティポリシーを実装するものとする。

オフプレミスの影響レベル 6 :

すべてのオフプレミス CSP のレベル 6 CSO は、SIPRNet (SIPRNet ネットワークエンクレーブ) または他の SECRET ミッションパートナーネットワークの拡張として扱われ、設計され、対処される。

IaaS/PaaS (VM および仮想ネットワークデバイスインターフェース) でインスタンス化され、SIPRNet に接続されているすべてのミッションオーナーのシステム/アプリケーションは、SIPRNet IP アドレスを使用してアドレスされる。これには、管理プレーンシステムとインターフェースを含む。

SIPRNet に接続されているすべてのオフプレミス CSP レベル 6 の SaaS サービスおよび一部の PaaS サービスは、SIPRNet に割り当てられ、管理されている SIPRNet IP アドレスを使用する必要がある。代替アドレッシングには免除の手続きが必要である。

オンプレミスの影響レベル 2/4/5 :

すべてのオンプレミスでレベル 2/4/5 IaaS/PaaS/SaaS CSO およびミッションオーナーシステム/アプリケーションは、DoD NIPRNet IP アドレスを使用して処置される。

オンプレミスの影響レベル 6 :

すべてのオンプレミスでレベル 6 IaaS/PaaS/SaaS CSO およびミッションオーナーシステム/アプリケーションは、DoD SIPRNet IP アドレスを使用して処置される。

5.10.4.2 ドメインネームサービス (DNS)

NIPRNet (および SIPRNet の .mil .mil DNS サーバー) 上の DoD .mil DNS サーバーは、DoD NIC およびサブテンディングされたコンポーネント NIC によって提供される DoD IP アドレスに対して権限を持っている。つまり、DoD の .mil DNS サーバーは .mil URL を宛先 IP アドレスとして名前解決を行う。NIPRNet の DoD .mil DNS サーバーは、特定の IP アドレスが関連付けられていない .mil URL をホストするためにも使用する必要がある。この場合、NIPRNet の DoD .mil DNS サーバーでは、CSO が使用する商用 URL を指すために CNAME が使用される。

NIPRNet 上の DoD .mil DNS サーバーは、DoD DNS プロキシ、エンタープライズ再帰サービス、DNSSec などのさまざまなセキュリティ手段を使用して保護されている。このような DoD DNS は多くの DNS 脅威から保護されており、DoD の DNS とそれに関連する保護サービスを DoD .mil URL とアドレス解決に適切に使用する必要がある。

一般規則、すべてのオンプレミスおよびオフプレミスの影響レベル 2/4/5 :

一般的には、DoDI8410.01 に従って、ミッションオーナーが IP アドレッシングを制御し、DoD NIPRNet IP アドレスを使用している IaaS/PaaS/SaaS CSO でインスタンス化された.mil ドメインを使用するミッションオーナーシステム／アプリケーションでは、パブリックや商用の DNS サーバーでなく、DoD の.mil NIPRNet の権威 DNS サーバーで.mil DNS レコードをホストする必要がある。したがって、そのようなミッションオーナーは、別のドメインを使用することが他に承認されない限り、CSP またはその他の非 DoD の DNS プロバイダによって提供される DNS サービスの利用を認定されない。

注：非.mil URL を使用するミッションオーナーは、運用を認められているドメインについて、CSP が管理しているか、または他の商用／パブリック DNS サーバ（DoD DNS サーバではない）を利用することができる。以上の一般規則に対し、次の例外が適用される。

オフプレミスで影響レベル 2 の例外：

既定で CSP が管理する商用 IP アドレスと URL を使用する、オフプレミスで影響レベル 2 の CSO を使用する DoD のミッションオーナーは、DoD の.mil NIPRNet DNS サーバーで.mil DNS レコードをホストし、商用 URL または IP アドレスを示すには、必要に応じて CNAME を利用しなければならない。CSP DNS サーバーは、商用 IP アドレス解決の権限を持つ。

オフプレミスで影響レベルの例外 4/5 SaaS および一部の PaaS：

オフプレミスの影響レベル 4/5 CSO（IaaS と一部の PaaS）を使用する DoD のミッションオーナーは、IP アドレッシングを制御できず、CSP が管理する商用 IP アドレスと URL に依存しているので、.mil DNS レコードを DoD の.mil NIPRNet DNS サーバーでホストし、商用 URL または IP アドレスを示すには、必要に応じて CNAME を利用しなければならない。CSP の DNS サーバーが商用 IP アドレス解決の権威を持つことになる。

それらの使用が必要な場合は、URL リダイレクションとダイナミック DNS ソリューションを含む CSP DNS サービスと、実装された DNS の保護が CSO の DoD PA に適したものとして評価され、承認される。CSP DNS サービスは DNS プロキシを使用して保護され、DNSSec をサポートする必要がある。DoD PA には、CSP の DNS 管理アーキテクチャまたはアウトソーシングサービスのリスクアセスメントも含まれる。

すべてのオンプレミスとオフプレミスで影響レベル 6：

オンプレミスまたはオフプレミスで影響レベル 6 の CSO を使用する DoD ミッションオーナーは、SIPRNet（または他の SECRET ミッションパートナーネットワーク）上の DoD の権威 DNS サーバーで DNS レコードがホストされる smil.mil URL を使用する。SIPRNet アドレスは、DoD NIC によって割り当てられる。

対応するセキュリティ管理策：SC-20、SC-21、SC-22

5.10.5 SaaS を使用したミッションオーナーの要件(全レベル)

CSP の SaaS アーキテクチャの保護／安全確保／防御は CSP の責任であるが、CSP の SaaS サービスを契約して使用するミッションオーナーは、DoD ポリシーを満たすために、最低限以下に対処しなければならない：

- プロトコルとサービスを、DoD PPSM レジストリの DISN を通過する SaaS サービスが使用する関連 UDP/TCP IP ポートとともに登録する。これには、レベル 4, 5, 6 のすべてのユーザおよび管理プレーントラフィック、および DoD ネットワーク内から管理または監視されている場合はレベル 2 の管理プレーントラフィックが含まれる。詳細はセクション 5.15 「ポート、プロトコル、サービス、管理とクラウド」を参照。
- トラフィックが IAP を通過する場合は、着信および発信トラフィックのサービス／アプリケーションを DoD DMZ ホワイティストに登録する。詳細は、5.17.2 「DoD DMZ ホワイティスト」を参照。

接続承認のための CSA の CSO を DISA SNAP データベースに登録する。これには、第 6 章「サイバー空間防御とインシデントレスポンス」で定義されているミッションサイバー防衛 (MCD:Mission Cyber Defense) アクションの実行のための認定 CSSP の指定も含まれる。

このステップは、DoD CSSP コミュニティが、セクション 5.18 「サプライチェーンリスクマネジメントアセスメント」に記載されているサイバー空間防衛の任務を遂行できることを認識・周知するよう、レベル 2 を含む SaaS のすべてのレベルで必要である (DISN とのプロダクション接続がない場合でも)。

セクション 5.10.3 「CSP サービスアーキテクチャ」で説明したように、ミッションオーナーは、DoD データ／情報の保護のための CSP とその SaaS 提供のセキュリティ態勢に依存している。

5.10.6 IaaS/PaaS を利用したミッションオーナーのシステム／アプリケーションの要件

ミッションオーナーは、IaaS/PaaS 上のシステム／アプリケーションを実装する際に情報の影響レベル全体にわたる縦深防御/防御策に対処する必要がある。(以下の情報を含むが、これに限定されない)

- VM 間、および VM と外部ネットワーク (物理および仮想の両方) 間のデータフローを制

御可能な、1 つまたは複数の仮想ネットワークに仮想マシン (VM) を実装する。

注：仮想ネットワークは、通常、VM をサポートする仮想化ハイパーバイザの機能である。

- DoD DMZ STIG、アプリケーションセキュリティおよび開発 STIG で定義されているアプリケーションタイプの承認されたアーキテクチャに従って、他のオペレーティングシステムおよびアプリケーション固有の STIG とともに仮想ネットワークを実装する。例えば、Web サービスやアプリケーションでは、通常、アプリケーション／データベースサーバーやその他のサポートしているシステム／サーバーの適切な保護とともに、インターネット／外部に面したサーバーや、プライベート／「バックエンド」ゾーンに対する適切な保護を備えた制限なし／制限付き DMZ ゾーンを備えた階層アーキテクチャを必要としている。
- ミッションシステム／アプリケーションがインターネットに接続されている場合は、DMZ STIG を使用して DMZ 保護の実装を行う（前述のゾーニングアーキテクチャに加えて）。たとえば、DMZ STIG には次のものが必要である（クラウドに適合した）。
 - パブリック仮想ネットワークゾーンの Web サーバー
 - プライベート仮想ネットワークゾーン内のアプリケーションサーバーとデータベースサーバー
 - 2 台のルータ（仮想クラウド用）：
 - ・ 外側—パブリックゾーンからインターネット
 - ・ 内部—パブリックゾーンからプライベートゾーンへ
 - リバース Web プロキシ (RWP)
 - FTP を使用する場合は FTP プロキシ
 - Web アプリケーションファイアウォール (WAF)
 - セキュリティ情報マネージャー (SIM)
 - Syslog サーバー
 - 2 つの Active Directory サーバー
 - ・ 公開ゾーン
 - ・ プライベートゾーン

影響レベル 2：DMZ 境界保護要件（すなわち、プロキシおよびファイアウォール）は、アプリケーションのミッション所有者によって実装されるか、DoD コンポーネントまたは DoD エンタープライズなどのより大きなエンティティによって提供される共通の境界サービスを活用する必要がある。これは、CSP 毎のベースで行われる可能性が高い。その他の一般的なサービスも利用可能である。

影響レベル 4 : DMZ 境界保護要件（すなわち、プロキシ、ファイアウォールなど）は、ミッションオーナーの機関またはエンタープライズサービスとして DISA によってそのような保護が提供されるまでは、そのシステム／アプリケーション環境でミッションオーナーによって提供される。

- インフラストラクチャがインターネットに直接アクセスする場合、仮想ネットワークと相互接続された VM を保護するために、該当する DoD SRG と STIG に従って、仮想アプリケーションレベルのファイアウォールと仮想侵入検知や防止機能の実装を行う。ミッションオーナーやその CSSP は、ファイアウォールルールを制御し、仮想ネットワークの境界を監視し、Tier 1 と同様に報告できる必要がある。DISN 接続（レベル 4～5）の専用インフラストラクチャの場合：ファイアウォール、IPS や仮想ネットワークから DISN 接続のインバウンド、アウトバウンドの制限するためのルーティングなどを DoDI 8551 に従って実装する必要がある。インターネットに接続されている可能性が最も高い CSP のネットワークなど、他のすべてのソースからのすべてのトラフィックのブロックを行う。
- 仮想ファイアウォール、仮想 IDS 機能、およびミッションシステム／アプリケーションを担当する CSSP 間で、安全な（暗号化された）接続またはパス（つまり、暗号化された VPN）を実装する。詳細については、第 6 章「サイバー空間防衛とインシデントレスポンス」を参照。
- IaaS : DoD のポリシーと CYBERCOM の指示に従って、各 VM の OS について、安全な設定（堅牢化/STIG）／パッチ／保守を行う。DoD STIG および SRG の使用は、IAVM への準拠と同様に安全な設定に必要である。
- PaaS : DoD のポリシーと CYBERCOM の指示に従って、ミッションオーナーの直接管理下にある CSP から提供された VM OS およびアプリケーション（CSP との契約ではない）に対して安全な設定（堅牢化/STIG）／パッチ／保守を行う。DoD STIG および SRG の使用は、IAVM への準拠と同様に安全な設定に必要である。
- IaaS/PaaS : DoD ポリシーと USCYBERCOM の指示に従い、ミッションオーナーが提供／インストールする各アプリケーションの安全な構成（堅牢化/STIG）／パッチ／保守を行う。DoD STIG および SRG の使用は、IAVM への準拠と同様に安全な設定に必要である。
- CSP の IaaS ストレージサービス製品に格納されているすべての DoD ファイルに対して、保存データ (data-at-rest) の暗号化を実装する。CSP は、これを達成するための 1 つ以上のサービスまたは方法を提供することができる。保存データの暗号化は、データ／情報の流出問題の緩和に役立つ。詳細は、5.11 項「商用クラウドストレージにおけるデータの暗号化・保護」を参照。

- DoD の情報が機微な政府の情報（FOUO や CUI など）である場合、FIPS モードで動作する FIPS 140-2 検証済みソフトウェア暗号化モジュールを使用する必要がある。
- 保存データの暗号化サービスは、ミッションオーナーが単独でキー管理と使用を制御できるように実装する必要がある。
- DoD のポリシーに基づいてホストベースのセキュリティシステム（HBSS: Host Based Security System）を実装する。
 - サポートされている汎用 OS に対し、すべての VM で HBSS エージェントを実装する。
 - NIPRNet 内の HBSS エージェント制御サーバー（EPO）または同じ CSO（例えば、VDMS）内の関連する共通仮想サービス環境を利用する。
 - HBSS エージェントとその制御サーバー間に安全な（暗号化された）接続またはパスを実装する。
 - 第 6 章「サイバー空間防衛とインシデントレスポンス」で定義されているミッションオーナーの CSSP エンティティによる可視性を提供する。
- USCYBERCOM TASKORD 13-670 に従って保証されたコンプライアンス・アセスメントソリューション（ACAS: Assured Compliance Assessment Solution）サーバーを使用してスキャンを実装する。
 - NIPRNet 内または関連する共通仮想サービス環境内の同じ CSO（たとえば VDMS）内の ACAS セキュリティセンターサーバーを利用する。
 - ACAS サーバーとその割り当てられた ACAS セキュリティセンター間に安全な（暗号化された）接続またはパスを実装する。
- 第 6 章「サイバー空間防衛とインシデントレスポンス」で定義されているように、ミッションオーナーの CSSP エンティティによる可視性を提供する。
 - 安全な接続を確立するための DoD PKI サーバー証明書を実装する。
- FIPS モードで動作する FIPS 140-2 検証済み暗号化モジュールを使用して、必要なすべてのデータ転送中の暗号化保護を実装する。
- DoD CAC/PKI 認証を次のように実装：
 - レベル 2、4、および 5 の VM オペレーティングシステムおよびアプリケーションへのすべての特権ユーザのアクセスは DoD のポリシーに従う。レベル 6 では、CNSS SIPRNet トークンを使用する必要がある。
 - レベル 4 および 5 の実装されたシステム／アプリケーションのすべての DoD の一般ユーザは DoD のポリシーに従う。レベル 6 では、CNSS SIPRNet トークンを使用する必要がある。
 - 実装されているシステム／アプリケーションと NIPRNet または SIPRNet 上の DoD OCSF レスポンダとの間に、適用可能な安全な（暗号化された）接続またはパス（つまり、暗号化された VPN）を実装する。
- Active Directory（AD）（使用されている場合）および関連する信頼の設定を、DoD

Windows OS STIG やその他の適用可能な DoD STIG に従ってセキュアーにする。これには、DoD AD フォレストと CSP CSO AD フォレスト間の信頼が含まれる。そのような信頼が必要な場合、実装は DoD AD フォレストを担当する A0 の承認を受けなければならない。詳細は、セクション 5.10.7「クラウドの Active Directory 統合」を参照。

- DISN を通過するプロトコルとサービスを、ミッションオーナーのシステム／サービス／アプリケーションで使用される関連する UDP/TCP IP ポートとともに登録する。これには、レベル 4, 5, 6 のすべてのトラフィック、およびレベル 2 の管理／監視プレーントラフィックが含まれる。詳細は、セクション 5.15「ポート、プロトコル、サービス、管理およびクラウドベースのシステム／アプリケーション」を参照。
- トラフィックが IAP を通過する場合は、インバウンドトラフィックとアウトバウンドトラフィックの DoD ホワイトリストにミッションオーナーのシステム／サービス／アプリケーションを登録する。詳細は、セクション 5.17.2「DoD DMZ ホワイトリスト」を参照。
- ミッションオーナーのシステム／サービス／アプリケーションと CSP の CSO を DISA SNAP データベースに接続認証のために登録する。これには MCD アクションを実行するための認定 CSSP の指定を含む。このステップは、DoD の CSSP コミュニティが、第 6 章「サイバー空間防衛とインシデントレスポンス」で説明した任務を実行できることを認識し情報が得られるよう、レベル 2 を含む IaaS/PaaS のすべてのレベル（DISN とのプロダクション接続がない場合でも）で必要である。
- DoD で使用されるすべての CSP の問題を監視するためのサイバー空間防御とインシデントレスポンスを実装する。

注：CSP がミッションオーナーの VM、OS、アプリケーションを安全に設定（ハード/STIG）／パッチ／維持する契約を結んでいる可能性のある PaaS（および潜在的に IaaS）の下で、STIG およびパッチされた VM イメージを使用するためには、適用可能なすべてのポリシー（例えば、特権アクセス）に基づいて DoD 基準に対して検証されなければならない。ミッションオーナーが CSP を契約して OS とアプリケーションを安全に設定する場合、CSP は該当するすべての DoD STIG を遵守することが期待される。IAVA 準拠の場合、CSO は、DoD の IAVA で参照される CVE で特定されたパッチを適用することにより、業界のベストプラクティスに準拠することが期待される。等価性は、ケースバイケースで評価され承認される。

5.10.7 クラウドの Active Directory 統合

Active Directory (AD) の実装 (必要な場合) は、Active Directory ドメインとフォレスト STIG⁹²で、クラウドサービスに関連する以下のガイダンスと共に構成される。

- オンプレミスのプライベート/コミュニティ (例: milCloud) の DoD/商用 CSP CSO 管理の AD :
 - AD サーバーとフォレストは、DoD ガイドラインを定めて、他の DoD 管理対象の AD サーバーとフォレストと信頼関係を確立することができる。
- オンプレミスのプライベート/コミュニティの IaaS/PaaS (例: milCloud) の DoD/商用 CSP CSO 管理の中にインスタンス化された DoD ミッションオーナーが管理する AD :
 - AD サーバーとフォレストは、確立した DoD ガイドラインに従って、他の DoD 管理の AD サーバーとフォレストと信頼を確立することができる。
- 商用オフプレミス IaaS/PaaS でインスタンス化された DoD ミッションオーナー管理の AD :
 - DoD AD フォレストは、商用 IaaS/PaaS でインスタンス化されたミッションオーナー管理の AD サーバーまたはフォレストを信頼しない。
 - AD サーバーとフォレストは、確立した DoD ガイドラインに従って、他の DoD 管理 AD サーバーとフォレストを信頼することできる。この信頼は一方通行でなければならない。次のサブセクションで説明するようなダイレクト信頼以外の方法を使用する必要がある。

注: これにより、商用 CSO で、侵害されたミッションオーナーの AD が DISN 上の DoD AD を侵害する可能性が軽減される。

- 非 DoD CSP CSO 管理の AD :
 - 非 DoD の CSP の AD は、CSO が不可欠な部分である場合、CSO にアクセス制御サービスを提供するために使用することができる。(例えば、SaaS の場合)
 - DoD AD フォレストは、非 DoD CSP の AD サーバーまたはフォレストを信頼しない。
 - 絶対に必要な場合のみ、非 DoD の AD フォレストが DoD の AD フォレストを信頼する可能性がある。この信頼は一方通行でなければならない。次のサブセクションで説明するようなダイレクト信頼以外の方法を使用する必要がある。

注: これにより、侵害された CSP の AD が DISN の DoD AD を侵害する可能性が軽減される。

⁹² Active Directory Domain and Forest STIGs:
<http://iase.disa.mil/stigs/os/windows/Pages/active-directory.aspx>

注：AD 実装のための DoD ガイドラインは、上記の AD ドメインとフォレスト STIG に記載されている。

5.10.7.1 Active Directory フェデレーションサービス (ADFS)

Active Directory フェデレーションサービス (ADFS) は、CSP の SaaS CSO などの別の組織にある Web サーバーに対して、社内の Active Directory アクセス制御資格情報の使用とシングルサインオン (SSO) 機能を拡張するために使用される。この機能により、1 つのブラウザセッションの存続期間中に複数の Web アプリケーションへのアクセス制御が可能になる。これは、IaaS/PaaS CSO でインスタンス化されたミッションオーナー自身の Web アプリケーションに SSO 機能を提供する場合にも、仮想環境に AD サーバーを配置することなく適用できる。本質的に ADFS は、CSP の CSO または外部ウェブアプリケーションが DoD AD に代わって主張された DoD のアイデンティティ請求を信頼することを可能にするので、ADFS の使用は上記の AD 要件の意図を満たしている。

5.10.7.2 Active Directory DirSync (ディレクトリ同期)

Active Directory DirSync は、特定の Microsoft SaaS CSO に固有の Microsoft Azure ツールである。DirSync は、ドメインに参加したサーバー（オンプレミスまたは Microsoft Azure VM）にインストールされ、オンプレミスの Active Directory ユーザをプロフェッショナルおよび小規模企業向けの Office 365 に同期させる⁹³ようになった。このツールは Office 365 AD にプッシュとしてユーザ情報を提供するため、Office 365 AD を使用してこれらのユーザの CSO へのアクセスコントロールを提供している。このツールは、前述の非 DoD の CSP 管理 AD 要件の目的を満たす。

5.11 商用クラウドストレージにおけるデータの暗号化・保護

すべての影響レベルのミッションシステムでは、DoD の保存データを DoD が専属的に統制する暗号化鍵と鍵管理により、暗号化する機能が必要である。一部の CSO は、ハードウェアセキュリティモジュール (HSM:Hardware Security Module) を提供するか、顧客専用の HSM デバイスをサービスとして提供することで、これを実現している場合がある。そのような機能を提供しない CSO は、ミッションオーナーが DISN 上で暗号化ハードウェア/ソフトウェアを使用することを要求するか、または DoD が統制する鍵および鍵管理のクラウド暗号化サービスを要求することができる。

顧客が統制する鍵と鍵管理による保存データ (DAR:Data-at-Rest) 暗号化は、CSO に格納されている DoD データを保護し、次の利点を持つ。

- 機密性が問題とならないレベル 2 で公開されている情報とウェブサイトの完全性の維

⁹³ DirSync: <https://technet.microsoft.com/en-us/library/dn635310.aspx>

持

- レベル 4 とレベル 5 の CUI の機密性と完全性を維持し、次の利点を有している。
 - 暗号化されていない DoD データを侵害／アクセスするために必要な作業を増やすことにより、CSP 要員による不正アクセスの内部脅威ベクトルを限定する。
 - 暗号化されていない DoD データを侵害／アクセスするために必要な作業を増やすことにより、ハッカーによる不正アクセスの外部脅威を限定する。
 - CSP の関与や協力なしの暗号の消去とファイルの削除を行うことにより、CSP オフホーディングに対する保証の高いデータ破壊を可能にする。
 - CSP の関与や協力なしの暗号の抹消とファイル削除により、高保証でデータ流出対処を可能にする。
 - 詳細は、セクション 5.11.1 「暗号の消去」を参照。

注：ミッションオーナーとその AO は、情報の完全性を維持する利点に加えて、レベル 2 でのデータ破壊や流出対処のための DAR 暗号化の利点を考慮する必要がある。

すべての情報影響レベル：

- すべての保管データ（DAR）を暗号化する：
 - 仮想マシン仮想ハードドライブに保管または
 - ブロックレベルまたはファイルレベルの大容量記憶装置／サービスに保管
 - データベースレコードに格納（PaaS、SaaS の場合、MO は DB と DBMS を単独で制御できない）
- すべての CUI の保護に関する連邦政府の方針・基準に従って、FIPS モードで動作する FIPS 140-2 検証済み暗号化モジュール⁹⁴（少なくともレベル 1）を使用する。
 - 暗号化モジュールには、暗号アルゴリズム、RNG、KMI、HASH など（承認されたすべての機能）を含む。
- CSP の顧客／ミッションオーナー（MO）は、作成から保管、使用、廃棄までの鍵の管理を維持する。
 - 必要に応じてハードウェアセキュリティモジュール（HSM）または鍵管理サーバーを実装して、DISN 内に鍵を格納、生成、管理する。
 - または、顧客／MO によってのみ管理される専用 HSM を提供する CSP サービスを発注する。

⁹⁴ NIST FIPS CMVP: <http://csrc.nist.gov/groups/STM/index.html>
<http://csrc.nist.gov/groups/STM/cmvp/index.html>

DoD キー制御による DAR の暗号化が不可能なクラウドアプリケーションの場合、ミッションオーナーはデータを CSO に転送する前に、関連するデータ所有者とリスク分析を実行する必要があります。この分析では、アプリケーションの終了時および CSO オフボード時にデータの流出を修正したり、データを確実に破棄したりするために利用できる保証の高い方法はないことを考慮する必要があります。ミッションオーナーの AO は、これらのリスクを受け入れる責任がある。

注：CSP の CSO DAR 暗号化機能とミッションオーナーの DAR 暗号化要件をサポートする能力は、DoD の PA の獲得に向けて評価され、文書化される。

対応するセキュリティ管理策：SC-28、SC-28 (1)

5.11.1 暗号消去

暗号の消去については、NIST SP 800-88 Rev 1⁹⁵で説明されている：

「暗号の消去は、データがメディアに格納されているときに暗号化される場合に使用できる新しいサニタイズ技術である。CE では、暗号化されたデータそのものを含むメディア上の保管箇所をサニタイズするのではなく、データを暗号化するために使用された暗号化キーをサニタイズすることによってメディアのサニタイズが行われる。CE の技術は、典型的には、媒体を非常に素早くサニタイズすることができ、部分的なサニタイズである記憶媒体のサブセットがサニタイズできる技術をサポートすることができる。選択的サニタイズと呼ばれることもある部分サニタイズは、クラウドコンピューティングにおいて潜在的な用途を有している。」

SP 800-88 の CE ガイダンスの多くは自己暗号化デバイスに関連しているが、このセクションでは、CE がクラウドコンピューティングに適用可能であることの NIST の認識を拡張している。

DAR 暗号化は、顧客による暗号キー管理の独占的な管理と相まって、DoD が CSP 支援や協力なしにデータを暗号的に消去する機能を提供している。この機能は、標準の CSP 提供のデータ削除と組み合わせて、上記セクション 5.11 の DAR 暗号化で説明した次の利点をもたらしている。

⁹⁵ NIST SP 800-88:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

データの削除とは、ファイルシステムおよびデータベースで使用する通常のファイルまたはデータレコードの削除方法を指す。暗号消去の前または後の削除で、リソースが CSP に復元され、通常の操作でデータを最終的に上書きすることができる。

暗号の消去とそれが提供するさまざまな利点をサポートするために、DAR 暗号化は適切なレベルの細かさで実行する必要がある。つまり、1 個のキーだけで、ミッションオーナーのデータのすべてまたは大部分を暗号化すべきではない。

関連セキュリティ管理策：MP-6 (3)、MP-6 (8)

5.12 バックアップ

CSP は、CP-9 セキュリティ管理策と一致する CS0 内のデータのバックアップを提供する責任を持っている。ミッションオーナーは、CP-9 との整合性を維持してデータを確実にバックアップする責任がある。しかし、ミッションオーナーは、データを単一の非 DoD CSP に委ねるリスクも考慮する必要がある。セクション 5.8 「CS0 からの移行のためのデータの処理と破壊」は、CS0 のシャットダウンの場合に、短期間でデータを回復や移行する準備ができていないミッションオーナーの重要性を論じている。

この準備は、CSP のバックアップ要件とともに、低～中程度の影響値の DoD データに対しては十分である。ただし、影響度の高いデータを持つミッションオーナーは、定期的にデータをバックアップし、DoD 所有のインフラストラクチャ／メディアや別の CSP が提供するクラウドストレージサービスに保存することを検討する必要がある。

異なるプロバイダに格納されたバックアップは、CS0 の業務停止や CSP のインフラストラクチャ全体に影響を与える致命的なイベントの場合に、データ損失／破損のリスクを低減する。そのようなバックアップのメンテナンスは、データ漏洩対処によるデータ損失のリスクを軽減することもできる。ミッションオーナーは、CP-2 セキュリティ管理策で必要とされる緊急時対応計画の一部として、そのようなリスク軽減の必要性を判断しなければならない。

注：IaaS/PaaS バックアップの場合、このセクションで使用されている「データ」には、VM のスナップショットまたは仮想ハードドライブを含む完全構成の VM のイメージが含まれているため、計算上の復元は処理される情報の復元と同じくらい簡単である。

注：このセクションは、ミッションオーナーによる検討のために提供されている。CSP や DoD PA の評価には影響しない。

対応するセキュリティ管理策：CP-2、CP-9

5.13 DoD 請負業者／DoD コンポーネントミッションパートナーによるクラウドサービスの利用

このセクションは、DoDIN.mil の一部ではないネットワークを持つ Non-CSP DoD 請負業者またはミッションパートナー（防衛産業基地（DIB Defense Industrial Base：）請負業者など）と DoD コンポーネントミッションパートナー（例：カミサリー、交換所、教育機関など）ドメインを対象としている。これらのミッションパートナーとそのネットワークのドメイン名は、通常、.gov、.org、.com、.edu である。

クラウドサービスを使用する場合、ミッションパートナーおよび請負業者は、DISN 提供の機能（CAP など）またはエンタープライズサービスに固有ではない、ミッションオーナーに関するこの CC SRG のすべてのガイダンスに従う責任がある。処理中の DoD データに基づいて、適切な影響レベルを選択する必要がある。ミッションパートナーと請負業者の内部ネットワークと CSP 間で転送されるすべての DoD データについて、暗号化による信頼できる通信手段を利用する必要がある。ミッションパートナーと請負業者は、適切な DoD のデータ所有者または指定された機関（DSS など）と協力して、CSO で発生するインシデントの対処手順を作成する責任も負っている。

注：以下に使用される「Non-CSP DoD 請負業者」という用語には、CSP ではなく、CSO（すなわち、インテグレータ）を集約してクラウドサービスの契約を履行する DoD 請負業者は含まれない。このように、この CC SRG の他の箇所に記載されているように、これらの Non-CSP インテグレータが下請けを介して提供している CSO は、CSO および DoD のそれらの使用に関するガイダンスに従わなければならない。

5.13.1 DoD コンポーネントミッションパートナー

.gov、.org、.com、.edu ドメインの DoD コンポーネントのミッションパートナーは、CSP/CSO によって処理／保存／送信する情報に関する CNSSI 1253 分類と最もよく一致する情報影響レベルの DoD PA を持つ CSP または CSO のみを使用する必要がある。情報がパブリックの場合は、インターネットに直接アクセスするレベル 2 の CSO が使用される。そうではなく、レベル 4/5 サービスにアクセスする場合は、組織のネットワーク／エンクレーブがどのように接続されているかによって異なる。これを以下に示す：

組織のネットワーク／エンクレーブ：

- NIPRNet の一部；CSO への接続は NIPRNet BCAP を経由

- ミッションパートナーの一部またはBCAPを介したCOIネットワーク;CSOへの接続は、そのBCAPを経由
- 1つ以上の承認された組織のIAPを介してインターネットに直接接続;CSOへの接続は、インターネットまたはプライベートな直接接続を介して行われる。このような接続は、クラウド内の組織のネットワークや情報/アプリケーションを保護するために適切に保護される。CSPのネットワークと組織のネットワーク境界はBCAPとみなされ、特定の組織のネットワークやその情報の保護に必要な境界保護と監視を行う。DoDコンポーネントのミッションパートナーは、ネットワークに対して適切な境界保護を実装する責任がある。

5.13.2 Non-CSP DoD 請負業者およびDIBパートナーによるCSPの利用による機密情報の保護

Non-CSP DoD 請負業者およびDIBパートナーは、クラウドサービスの提供に関連しないDoD契約と併せて、DoDIN以外の重要なDoDデータ/情報を保存、処理、使用または作成することがある。そのような請負業者は、格付けされていないセンシティブなDoDデータ/情報がその環境にある間は（すなわち、DoDのCUIを保管し、請負業者の機能のサポートを行う請負業者に利用され、請負業者が所有/運用するITシステム）、主として機密性に焦点を当てたDoD 8582.01「DoD以外の情報システム上の格付けの無いDoD情報のセキュリティ」⁹⁶とNIST SP 800-171「連邦政府の情報システム外のシステムや組織におけるCUI情報の保護」⁹⁷に従って保護する必要がある。

Non-CSP DoD 請負業者およびDIBパートナーは、契約の履行または所有するDoDデータ（CUIまたは保護された防衛情報（CDI: Covered Defense Information））の保護/処理のためにクラウドサービスを利用する場合がある。したがって、センシティブなCUI/CDIの保護のために、Non-CSP DoD 契約者はDoDのレベル4 PAを付与されたCSOを利用することが強く推奨されている。そのようなCSOはNIPRNetだけに接続されている、DoD専用ではないことを意味している。つまり、CSP/CSOへのアクセスは、インターネットまたはプライベートな直接接続を介して行われる。NIPRNetは接続パスとして使用されない。DoDの請負業者は、ネットワークの適切な境界保護とクラウドに置かれた情報の保護を実装する責任がある。

⁹⁶ DoDI 8582.01: <http://www.dtic.mil/whs/directives/corres/pdf/858201p.pdf>

⁹⁷ NIST SP 800-171:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf>

DoDがこのレベル5の制限を変更するまで、Non-CSP DoD 契約者およびDIBパートナーは、そのような契約者が連邦政府機関のサポートされていないコミュニティの外にいるため、DoDのレベル5 PAを付与されたCSOを利用することはできない。

注：Non-CSP DoD 請負業者とDIBパートナーは、CDIの保護のためにNIST SP 800-171を遵守する必要がある。DoD レベル4 およびレベル5のベースラインは、CM-3 (2)、CM-7 (4)、およびIR-2 (1)を除き、SP 800-171で参照されるC/CEのすべてをカバーしている。

5.13.3 Non-CSO 製品またはサービスの一部として Non-CSP DoD 請負業者の CSP の利用

Non-CSP な DoD の請負業者は、契約された Non-CSO 製品またはサービス（例えば、兵器システムまたは主要アプリケーション）のコンポーネントとして第三者の CSO との統合を選択することができる。そのような請負業者は、CSP/CSO によって処理／保存／送信される情報の CNSSI 1253 分類に最もよく合致する情報影響レベルに対応した DoD の PA を有する第三者の CSP または CSO のみを利用することができる。さらに、CSO とその利用については、可能な限り DISN 提供の機能（例えば、CAP）またはエンタープライズサービスに特有ではない、ミッションオーナーに関する CC SRG ガイダンスに従わなければならない。CSO への接続は、契約された製品またはサービスが使用される場所とこの CC SRG の関連ガイダンスによって決定される。たとえば、製品またはサービスが NIPRNet ベースで、情報影響レベルが4または5の場合は、NIPRNet BCAPを使用する必要がある。情報影響レベルが2の場合は、インターネットを使用することができる。すべての CC SRG 要件が製品に適用され、さまざまな DFARS 条項に従い、下請けの CSO にも適用される。

Non-CSP DoD 請負業者が CSO を自ら提供しホストすることを選択した場合、CSO によって処理／保存／送信される情報の CNSSI 1253 分類に最も合致する情報影響レベルの CC SRG 要件が適用される。CSO が製品に専念する場合、A&A は通常の DoD 契約の A&A に従って取り扱われる。この場合の DoD PA の付与に関する考慮事項は、A&A プロセスの結果、CC SRG の遵守、および他の DoD のミッションオーナーが CSO を使用する可能性に依存している。

5.14 ミッションオーナーの DoD テストとクラウド上での開発

クラウド環境は、ミッションオーナーがアプリケーション開発やテスト、研究を行うのに適している。さらに、クラウドベースアプリケーションのアプリケーションライフサイクル管理に関連するテストおよび開発活動は、運用アプリケーションと同じ環境で実行するのが最善である。このセクションでは、ミッションオーナーが環境を管理している IaaS および PaaS の CSO の DoD テストと開発（T&D: Test and Development）活動について説明している。

DoD の T&D と試験環境のセキュリティ要件は、エンクレーブ T&D STIGs⁹⁸スイートで定義されている。最新のガイダンスについては、IASE の STIG を参照のこと。CC SRG のこのセクションは、各ゾーンに関連付けられたセキュリティ要件を変更するものではないが、クラウドで動作しているときの特徴を追加している。クラウドでインスタンス化されたすべての T&D ゾーンは、ここに追加された微妙な違いのあるリモートアクセスガイダンスを除いて、これらの STIG に準拠する必要がある。

エンクレーブ T&D STIG 概要文書では、4 つの T&D ゾーンが定義されている。これらのゾーンについて簡単に説明する。

- ゾーン A : 実稼働環境に導入する前の最終段階のテストのための、アプリケーションライフサイクル管理の手段。この環境は、運用ネットワークに接続され、アプリケーションをサポートする最終的な運用環境を再現している。開発者と管理者のためのリモートアクセスのための VPN が実装されるかもしれないが、検査のための T&D DMZ で終了しなければならない。環境内の資産は、STIG および IAVM 準拠を含めるために本番環境と同様に保護される。最終的なテスト段階で、最終的な改訂と小幅な更新など最小限の開発は許容される。

注 : Zone A は、DOT&E (Director, Operational Test and Evaluation) および JITC (Joint Interoperability Test Command) が DoD のアプリケーションとシステムについて DoD の試験・評価 (T&E) を実行する環境をサポートしている。

- ゾーン B : コーディング、コンプライアンス、テストなどのアプリケーション開発アクティビティのアプリケーションライフサイクル管理の支援。この環境では、実稼働ネットワークを保護してアプリケーションテストを行うためのアクセスコントロールを備えた運用ネットワークへの接続を提供している。プロダクション環境では許可されないアプリケーション開発を容易にするツールと機能を利用するため、独立したネットワークセグメントを提供している。開発者と管理者の環境のテスト・セグメントへのリモートアクセスを実装している。WRT (Wide Area Router/Transport) STIG および IAM の裁量による IAVA の遵守で、セキュリティが確保されている。
- ゾーン C : DoD 運用ネットワークに接続されていないクローズドテスト環境であるが、直接接続またはトンネリングメカニズムを使用して複数のテスト環境を相互接続している。この環境は、長距離ネットワーク接続を必要としていて、DoD 運用ネットワークを脅かす可能性のあるセキュリティの体制や危険性が不明であるか、または危険であ

⁹⁸ T&D STIGs: http://iase.disa.mil/stigs/net_perimeter/enclave-dmzs/Pages/index.aspx

る可能性があるシステム、デバイス、アプリケーション、ツールやプロトコルのテストに使用できる。

- ゾーン D : DoD のポリシーで禁止されていない範囲で、禁止されたツールを使用し、制限されたポート、プロトコル、およびサービス (PPS) を使用した悪意のあるコードやウイルスサンプルの操作を目的とした広範なテストを行う DoD ライブ運用ネットワークとは完全に閉じた物理的に別個のネットワーク。この環境内での開発は、一般的に推奨される方法ではない。

クラウドインフラストラクチャで実行されるすべての DoD テストと開発は、エンクレープ T&D STIG 概要文書の T&D Zone の記述に従って分類され、関連するエンクレープ T&D STIG のセキュリティ要件を遵守しなければならない。

ゾーン A とゾーン B は、アプリケーションライフサイクル管理に役立ち、運用ネットワークに接続できるため、これらのゾーンは、サポートする運用アプリケーションと同じ IaaS/PaaS クラウドインフラストラクチャに実装するのが自然である。現在の仮想ネットワークに特有の、堅牢なルーティングとフィルタリング機能により、VLAN または個別の仮想ネットワークを使用して、関連するゾーン A および B の STIG 要件に基づいて、これらのゾーンのセグメント化は容易に実装可能である。

アプリケーションライフサイクル管理には、通常、アプリケーション開発ゾーン B、アプリケーションテストゾーン A、および運用ゾーンが含まれる。各ゾーンには独自のサイバーセキュリティ要件があり、ゾーン自体と DoDIN を保護するための実装が必要である。DoD 運用アプリケーションと同様に、T&D ゾーン A および B は、NIPRNet に接続された DoD プライベート I/PaaS CSO でインスタンス化される。T&D ゾーン A と B も、同じ CSO に実装されている場合、運用ゾーンと同じ CSSP によって保護され監視されなければならない。

DoD のアプリケーション・テスト・クラウド・インフラストラクチャでインスタンス化されたゾーン A は、同じ情報影響レベルを持ち、アプリケーションのライフサイクル管理をサポートするために運用アプリケーションゾーンと同じ接続モデルを持つ同じ CSP/CSO で実装する必要がある。運用アプリケーションによって処理される情報の機密性は、この SRG に従って、CSO とその PA の情報影響レベルを決定する。アプリケーション開発者の所在地に基づき、いくつかの例外があるかもしれないが、これは運用アプリケーションのライフサイクル管理に使用される場合は DoD アプリケーション開発ゾーン B にも当てはまる。同じ接続モデルと CSSP を運用アプリケーションゾーンとして使用して、3 つのゾーンをすべて同じ CSO に配置することにより、クラウドの効率化を実現し、アプリケーション、処理される情報や DoDIN のより良い保護が可能となる。

DoD アプリケーションの開発クラウドインフラストラクチャでインスタンス化されたゾーン B は、開発者がインターネット経由でゾーンにアクセスする前に、プロダクション前のアプリケーション開発をサポートするレベル 2 PA を持つ CSP の CSO に実装する必要がある。この目的のため、レベル 4/5 の CSO にゾーン B を実装する際の考慮事項は、アプリケーション自体の機密性とそのコードに依存する。これは、プログラムの IAM または責任ある AO の裁量に委ねられている。ここでまた、開発が完了し、ゾーン B を運用アプリケーションのライフサイクル管理に使用する場合は、運用アプリケーションと同じ CSP/CSO に実装する必要がある。ゾーン B 内のシステムは STIG に準拠する必要はなく、ゾーン A または運用ゾーンと同じ HBSS および ACAS 要件を満たすべき対象ではないが、ネットワークインフラストラクチャとネットワークトランスポートは STIG 準拠でなければならない。これには、適切に堅牢化されたゾーン境界スタックが含まれており、ゾーン内の安全性が低い領域を保護する。この境界は、CSSP によって監視され、保護されなければならない。

ゾーン C および D は一般的に物理的な設備で実装されているが、さまざまな側面で仮想化を使用でき、これらのゾーンは、DoD 運用ネットワークに必要な接続性を提供しないクラウドサービスのみで実装できる。これにより、NIPRNet に接続されたオンプレミス CSO は、現在設計されているような milCloud などの複数の DoD テナントによる幅広い使用を目的としている。

代わりに、ゾーン C や D は、DoD ネットワークに直接接続されていないオフプレミスの商用、またはオンプレミスの DoD クラウド環境で、CSP の CSO やネットワーク、他の CPS のテナントのシステム/アプリケーションまたはインターネットに対して脅威とならないテスト活動を提供するよう実装されている。これらのユースケースに対する追加の例外や要件が、このリリースまたは別の SRG の将来のリリースで提供される可能性がある。レベル 4/5/6 として分類され、オンプレミス CSO で実装されるゾーン C と D は、DISN に接続することはできない。すなわち、これらのゾーンは BCAP を介して接続していない。ゾーン C と D は、CSSP によって監視・保護される場合とされない場合があるが、インシデントレポートを受信してインシデントレスポンスを行うよう、CSSP が調整する必要がある。

対応するセキュリティ管理策：CM-4、CM-4 (1)

5.14.1 クラウドベースの T&D ゾーンへのワークステーションの接続性

クラウドでインスタンス化されたすべての T&D ゾーンへのワークステーション接続は、クラウドの特徴から、結果としてリモート接続を使用する。異なるゾーンには、異なるタイプのワークステーションとリモート接続モデルが必要である。オプションは次のとおり。

- アプリケーションテストゾーン A は、運用アプリケーションと同じ方法でアクセスされる。
 - ワークステーションは NIPRNet に接続されている。運用アプリケーションと同様に、環境の管理とアプリケーションをテストするには、STIG に対応した官給品 (GFE: Government Furnished Equipment) を使用する必要がある。
- アプリケーション開発ゾーン B 接続：
 - ゾーン B は、運用アプリケーションのライフサイクル管理のサポートを行う、関連したゾーン A と運用ゾーン（商用のオフプレミスまたは DoD プライベートオンプレミス）と同じ CS0 の中である。
- 開発用ワークステーションが NIPRNet に接続されている場合は、運用アプリケーションと同様に、STIG に対応した官給品を使用して環境を管理し、アプリケーションをテストする必要がある。リモートターミナルソリューション（例えば、Citrix、ターミナルサービス（要塞ホスト））を使用することができる。VPN は機密データのトンネリングにのみ必要である。
 - ゾーン B は、関連するゾーン A と運用の前段階のアプリケーションの開発をサポートする生産ゾーンとは別の CS0 の中である。
- オフプレミスで契約された開発者で、商用オフプレミス CS0：VPN または暗号化されたプロトコルを使用したインターネット接続では、官給品以外を使用できる。
- オンプレミスの DoD または契約した開発者で商用オフプレミス CS0：ゾーン B は、自前のファイアウォールの背後に設定する必要がある。ゾーンにアクセスするには、VPN を使用する必要がある。NIPRNet 接続のためには、STIG 対応の官給品を使用する必要がある。ゾーン内のシステムのウィンドウ表示から、ローカル WS が侵害されることのないように、ゾーン B 環境に VPN が確立された後、遠隔端末ソリューション（例えば、Citrix、T ターミナルサービス（要塞ホスト））も必要である。パスは、IAP/インターネットまたは BCAP/プライベート接続を経由する。
- T&D/研究ゾーン C および D：
 - 通常、ゾーン D にアクセスするワークステーションは、ゾーン内から、またはゾーン C に構築された接続ゾーン D からアクセスする必要がある。クラウドは、次のようないくつかのシナリオを提示している：
- ゾーン D またはゾーン C のすべての部分がインターネットに接続され、CS0 がインスタンス化：ワークステーションはインターネット経由で接続する。NIPRNet 接続は、VLAN、VRF や VPN を使用する専用ネットワークまたはセグメント化した NIPRNet パス経由で接続する専用ハードウェアを除いて、一般的に排除される。
- ゾーン C に構築された 1 つまたは複数のゾーン D エンクレープで、DoD プレミスの物理ゾーン D エンクレープ：ゾーン C のすべての部分は、オフプレミス CS0 で実装された

部分を含めて、ゾーン C 内のワークステーション（すなわち、物理的なゾーン D エンクレープ）からアクセスする必要がある。このシナリオでは、ゾーン D または C の外部からのリモートアクセスは必要とされない。

5.15 ポート、プロトコル、サービス、管理およびクラウドベースのシステム／アプリケーション

任意のサービスタイプ（I/P/SaaS）の CS0 を利用するミッションオーナーは、IaaS/PaaS CS0 でシステム／アプリケーションを実装して操作する場合または SaaS の提供を利用する場合、DoDI 8551.01「ポート、プロトコルとサービス管理」（PPSM:Ports, Protocols, and Services Management）⁹⁹に従わなければならない。DoDI 8551.01 は、DoD のミッションオーナーが CM-7、CM7（1）、および SA-9（2）に準拠するためのポリシーのガイダンスを提供する DoD のポリシーである。CSP は内部ネットワークとサービス提供のために、これらの C/CE に準拠する必要があるが、DISN を通過するプロトコルとサービス（PS:Protocols and Services）にポリシーが適用されるため、DoDI 8551.01 は CSP には適用されない。

DISA PPSM オフィス¹⁰⁰¹⁰¹は、PPSM 変更管理委員会（CCB:Change Control Board）および技術諮問グループ（TAG:Technical Advisory Group）と共に、特定の DISN 境界の通過が許可された PS と、各 PS に対する脆弱性評価（VA: Vulnerability Assessments）を一覧にした、カテゴリ割り当リスト（CAL:Category Assignment List）を発行している。CAL にリストされている VA への準拠は、PS を安全に利用する上で鍵となっている。言い換えれば、DISN 上で使用される PS は、関連付けられた VA に従わなければならない。ミッションオーナーは、システムを構築する際に、PPS VA に提示されている緩和策を活用する必要がある。さらに、すべてのミッションオーナーは、I/PaaS CS0 のシステム／アプリケーション、または使用している SaaS 製品を含め、DoD PPSM レジストリ（SIPRNet でのみ可）へクラウド CS0 ベースのシステム／アプリケーションを登録する必要がある。登録には、すべての PS と、DISN を通過するアプリケーションによって使用される UDP/TCP IP ポートが含まれる。これには、レベル 4,5,6 のすべてのユーザ、管理プレーントラフィック、および DoD ネットワーク内から管理または監視されている場合はレベル 2 の管理プレーントラフィックが含まれる。

CC SRG のこのセクションの残りの部分では、PPSM データベースにアプリケーションを登録する際の、ミッション所有者に対するガイダンスである。

⁹⁹ DoDI 8551.01: <http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf>

¹⁰⁰ PPSM Office IASE page: <http://iase.disa.mil/ppsm/Pages/index.aspx>

¹⁰¹ PPSM Office Public page: <http://disa.mil/network-services/Enterprise-Connections/PPSM>

レベル 2 のオフプレミス CS0: レベル 2 ミッションオーナーの IaaS/PaaS CS0 における仮想ネットワーク、仮想マシン、およびアプリケーションは、DoD エンクレーブを構成し、外部ネットワーク経由でアクセスされる。同様に、SaaS CS0 は、エンクレーブ内の領域であり、外部ネットワークを介してアクセスされる。この外部ネットワークはインターネットである。レベル 2 のミッションオーナーは PPSM 境界 1-5 の PPSM ガイダンスを活用する必要がある。これは、IaaS/PaaS の仮想ネットワークとシステム/アプリケーション、I/P/SaaS の CS0 管理トラフィックのミッションオーナーの管理トラフィックにのみ適用される。ミッションオーナーが、PPSM データベースにアプリケーションを登録する際、境界 1-5 に登録する必要がある。非特権ユーザトラフィックはインターネット経由で送信されるため、このトラフィックの一部が DoDIN 内の特権を持たないユーザとの間であっても、登録は必要ない。このようなトラフィックは、他のウェブベースのトラフィックと同様に DISN IAP を通過する。

注：このガイダンスは、PPSM CCB の決定を待っている間、ユーザプレーンのトラフィックに関して変更することができる。ミッションオーナーの仮想エンクレーブの境界にファイアウォールとセンサーが必要であり、ミッションオーナーのシステム/アプリケーションアプリケーションを保護する MCD によってセンサーが監視されるため、以下のレベル 4/5/6 について同じまたは類似のガイダンスが提供される適用される。

レベル 2/4/5/6 オンプレミス CS0: オンプレミス CS0 は、どのレベルでも通常の DoD エンクレーブとして扱われる。PPSM 登録は、直接接続されている場合は境界指定 7-11 を使用し、IPSEC トンネルを介して接続されている場合は 10-12 および 15 を使用する。

レベル 4/5/6 オンプレミス CS0: CC SRG に従って、レベル 4/5/6 オフプレミス CS0 は、外部ネットワーク（CSP のネットワーク）であり、BCAP を介して接続されているにもかかわらず、DoDIN/DISN の拡張として設計されているため、通常の DoD エンクレーブとして扱われる。このように、PPSM 登録は、直接接続されている場合は境界指定 7-11 を使用し、IPSEC トンネルを介して接続されている場合は 10-12 と 15 を使用する。

注：ローカルサービスとして指定された PS は、IaaS/PaaS CS0 のミッションオーナーのシステム/アプリケーション仮想領域内で、仮想領域の境界を横断しない他の領域と同様に使用できる。

5.16 モバイルコード

モバイルコードは、リモート情報システムから取得され、ネットワークを介して送信され、受信者による明示的なインストールまたは実行なしにローカル情報システム上で実行され

るソフトウェア・プログラムまたはプログラムの一部として定義される。モバイルコードの作成および使用のためのメカニズムを提供するソフトウェアテクノロジーとして、Java、JavaScript、ActiveX、VBScript などの例がある。

モバイルコードは、CSP と DoD のミッションオーナーの両方に多数の攻撃ベクトルを提供している。CSP 組織の IT システムおよび CSO をサポートするインフラストラクチャは、悪質なモバイルコードに対して脆弱であり、侵害された場合、DoD のミッションオーナーのシステム／アプリケーション／情報／データのセキュリティが悪影響を受ける可能性がある。さらに、CSO や DoD のミッションオーナーのシステム／アプリケーションが侵害されて、悪意のあるモバイルコードがこれらのシステムから提供される（ダウンロードされる）と、顧客のエンドポイントとネットワークに悪影響を与える可能性がある。

DoD のモバイルコードポリシーは改訂中であるが、CNSS と DoD は次のようなカテゴリでモバイルコードを認識している。

カテゴリ 1：ワークステーション、サーバー、リモートシステムのサービスおよびリソースへの無条件のアクセスを可能にする、幅広い機能を備えたモバイルコードテクノロジー。カテゴリ 1 のモバイルコードテクノロジーは、一旦実行するとほとんどまたはまったく対策ができない既知のセキュリティ脆弱性を引き起こす。

カテゴリ 2：ワークステーション、サーバー、リモートシステムのサービスとリソースへの仲介アクセスを可能にする完全な機能を備えたモバイルコードテクノロジー。カテゴリ 2 のモバイルコードテクノロジーには既知のセキュリティ脆弱性を引き起こすが、既知の細かい、定期的な、または継続的な対策／保護が存在している。

カテゴリ 3：機能が限定されており、ワークステーション、サーバー、リモートシステムのサービスおよびリソースへの無条件なアクセスはできないモバイルコードテクノロジー。カテゴリ 3 のモバイルコードテクノロジーは、既知のセキュリティ脆弱性を抱えている可能性があるが、既知のきめ細かい、定期的な、または継続的な対策／保護手段もサポートされている。

新興モバイルコードテクノロジー：機能と脅威レベルがまだリスク評価を受けておらず、上記のように分類されていない、モバイルコードテクノロジー、システム、プラットフォームまたは言語。

DoD モバイルコードポリシーの遵守の大半はミッションオーナーの責任であるが、SC-18 (2) では、「情報システムに導入されるモバイルコードの取得、開発、使用は、組織が定めたモバイルコードの要件に合致していることを保証する」としている。DoD IS には以下が適用されている。

(a) リスクアセスメントを受けておらず、CIO によってリスクカテゴリに割り当てられている新興のモバイルコードテクノロジーは使用されない。

(b) カテゴリ 1 のモバイルコードが、コード署名証明書で署名されている；未署名のカテゴリ 1 モバイルコードの使用は禁止されている。署名されていないモバイルコード (Windows Scripting Host など) をブロックまたは無効にすることができないカテゴリ 1 のモバイルコードテクノロジーの使用は禁止されている。

(c) システムリソース (例えば、Windows レジストリ、ファイルシステム、システムパラメータ、および発信ホスト以外へのネットワーク接続) にアクセスすることなく、制限された環境で実行されるカテゴリ 2 のモバイルコードは使用できる。

(d) 拘束環境で実行されないカテゴリ 2 のモバイルコードは、保証されたチャネル (例えば、SIPRNet、SSL 接続、S/MIME、コードが承認されたコード署名証明書で署名されている) から取得した場合には使用できる。

(e) カテゴリ 3 (限定された機能で、コンピューティングプラットフォームのサービスおよびリソースへの無作為なアクセスの能力を有さないモバイルコード) モバイルコードは使用できる。

DoD は、CSP が組織の IT システム、CSO、ミッションオーナーのシステム／アプリケーション／情報／データの保護のために、CSO をサポートするインフラストラクチャについて、SC-18 (2) と同様のモバイルコードポリシーを制定することを期待している。さらに、DoD は、CSP の CSO が、CSO のエンドユーザ、ミッションオーナー、エンドユーザのシステムおよびネットワークを保護するために、承認されていない／危険なモバイルコードのダウンロードを有効、または許可しないことを期待している。SC-18 (2) は、すべての影響レベルについて FedRAMP+ベースラインへの追加について検討中である。

同様に、SC-18 (3) および SC-18 (4) には表 9 の値が割り当てられている。これらは現在、SLA／契約に含めるためにミッションオーナーによって検討される SLA 管理策のセットである。これらも、すべての影響レベルについて FedRAMP+ベースラインへの追加について検討中である。

ミッションオーナーのシステム／アプリケーションは、上記で許可されている場合を除き、モバイルコードをダウンロードして実行してはならず、システム／アプリケーションの

エンドユーザおよびエンドユーザのシステムやネットワークを保護するために、承認されていない／リスクのあるモバイルコードのダウンロードを許可してはならない。

5.17 クラウドベースのシステム／アプリケーションの登録と接続承認

このセクションでは、セクション 5.15「ポート、プロトコル、サービス、管理、およびクラウドベースのシステム／アプリケーション」で説明した PPSM 登録に加えて、クラウドベースのシステム／アプリケーションに必要なさまざまな登録に関する情報を提供している。

5.17.1 DISA システム／ネットワーク承認プロセス (SNAP)

ミッションオーナーは、すべてのクラウドベースのシステム／アプリケーションを登録する必要がある。CSP/CSO、MCD および接続方法を DISA のシステム／ネットワーク承認プロセス (SNAP : Systems/Network Approval Process) ¹⁰²データベース・クラウドモジュールへ登録しなければならない。この登録は、これらのシステム／アプリケーションを DISN へ接続することを可能にし、DoDIN、DoD 情報、およびミッションオーナークラウドベースのシステム／アプリケーションの保護を担う、サイバーセキュリティ防衛コミュニティの状況認識にとって不可欠である。

5.17.2 DoD DMZ ホワイトリスト

DoD DMZ ホワイトリストの実装は、DoD DMZ プログラムの運用をサポートする USCYBERCOM の TASKORD 12-0371 およびそれに続く FRAGO をサポートしている。ミッションオーナーのクラウドベースのシステム／アプリケーションで、トラフィックが DISN IAP を通過する必要がある場合は、システム／アプリケーションの URL/IP アドレスを DoD DMZ ホワイトリストに登録する必要がある。通常、IAP を通過するトラフィックは、レベル 2、オンプレミスのシステム／アプリケーションのための管理トラフィック、およびインターネットに面しているレベル 4/5 システム／アプリケーションとのユーザ・プレーン・トラフィックである (つまり、DoD DMZ 拡張 BCAP に接続されている)。このようなトラフィックや IP アドレスは、ホワイトリストに登録されていないとブロックされる可能性がある。ホワイトリストの URL は SIPRNet 内の <https://niprdmzwhitelist.csd.disa.smil.mil/home.aspx> である。「ヘルプ」リンクから利用可能なホワイトリストユーザガイドを閲覧できる。ミッションオーナーは、DoD コンポーネントの連絡先に連絡して、ホワイトリストにエントリを追加する必要がある。

¹⁰² SNAP: <https://snap.dod.mil/gcap/home.do> Connection Approval:
<http://www.disa.mil/Network-Services/Enterprise-Connections/Connection-Approval>

5.17.3 選択とネイティブプログラミングデータ入力システム - 情報技術 (SNaP-IT)

DoD メモ「商用クラウド・コンピューティング・サービスの導入および使用に関するガイダンス」2014年12月15日に対応し、DoD コンポーネントはすべての適切な情報を報告しなければならない。各クラウドコンピューティングの利用に関する DoD CIO 年次 IT 予算ガイダンスで示された選択およびネイティブプログラミングデータ入力システム—情報技術 (SNaP-IT: Select and Native Programming Data Input System—Information Technology)¹⁰³の中のすべての適切な情報について報告を行う必要がある。SNaP-IT は、DoD の IT 予算の見積もりを議会に公開するために使用される信頼すべき DoD データベースであり、OMB Circular A-11 セクション 53 およびセクション 300 が情報技術について OMB に提示している。遵守するために、コンポーネントは、Exhibit 53 の SNaP-IT プロファイルの 2 種類の質問、Exhibit 53A「機関の IT 投資ポートフォリオサマリー」と Exhibit 53C「機関のクラウドコンピューティング支出サマリー」に応じなければならない。コンポーネントは、クラウドコンピューティングオプションが各投資に対して評価されたかどうかを判定し、指示どおりに詳細を提供する必要がある。コンポーネントは、各コンポーネント投資の SNaP-IT プロファイル、リソース、および予算サポートデータを完成することにより、すべての Exhibits 53 の要件を満たすことになる。

5.18 サプライチェーンのリスクマネジメントアセスメント

DoD は、SA-19 がコンポーネントの真正性を扱う一方、DoD は FedRAMP+管理策 SA-12 を選択してサプライチェーンリスクマネジメント (SCRM: Supply Chain Risk Management) に取り組んでいる。偽造品、信頼性の低い、または悪意のあるロジックやコードを含むシステムコンポーネントおよびソフトウェアの取得は、CUI および機密情報の処理、保管、送信をサポートするすべての製品について、DoD にとって大きな懸念事項である。この懸念はクラウドコンピューティングにも及ぶ。

CSP は、CSO の DoD PA 評価パッケージの一環として、CSP は偽造品、信頼性の低い製品、悪意のあるソフトウェアを取得していないことや、これらを CSO のインフラまたは管理プレーンに導入していないことを示す、サプライチェーンアセスメント/管理とコンポーネントの真正性のプロセスと対策の概要を記した SCRM 計画を提供する。

CSP が SA-12 と SA-19 をどのように実装するかについての CSP の SCRM 計画は、すべての影響レベル 4, 5, 6 において CSO の DoD PA 評価プロセスの中で評価され承認される。

¹⁰³ SNaP-IT U: <https://snap.pae.osd.mil/snapit/loginauth.aspx> for Levels 2/4/5 systems/applications

SNaP-IT S: <https://snap.cape.osd.smil.mil/snapit> for Level 6 systems/applications

5.19 TASKORD 12-0920 に従った電子メールの保護

米国 CYBERCOM のタスクオーダー (TASKORD) 12-0920 では、インターネットからのインバウンドまたはアウトバウンドへのすべての電子メールに対して、エンタープライズ E メールセキュリティゲートウェイ (EEMSG:Enterprise E-Mail Security Gateway) を使用する必要がある。さらに、EEMSG を通過するには、1 つの DoD コンポーネントの電子メールサーバーから別のコンポーネントの電子メールサーバーへ送信される電子メールが必要である。EEMSG はサーバー間の電子メールトラフィックのみを処理し、クライアントからサーバーへのトラフィックは処理しない。除外されない限り、すべての DoD のコンポーネントは EEMSG を使用する必要がある。除外された場合、DoD コンポーネントは独自の E メールセキュリティゲートウェイを使用する必要がある。

それゆえ完全に TASKORD に従えば：

- BCAP 経由で CSO 内のミッションオーナーのエンクレーブ内にある L4/5 電子メールサーバー宛ての外部電子メールサーバーから IAP を介して受信したすべての電子メール転送は、EEMSG インバウンド保護を通過する必要がある。
- BCAP を介し、CSO 内のミッションオーナーのエンクレーブ内にある L4/5 電子メールサーバーから、IAP を介して外部電子メールサーバーに送信されたすべての電子メール転送は、EEMSG アウトバウンド保護を通過する必要がある。
- CSO 内のミッションオーナーの領域にある L4/5 電子メールサーバーから、BCAP 経由で DoD コンポーネントのデータセンターエンクレーブ内の電子メールサーバーに送信されるすべての電子メール転送は、EEMSG アウトバウンド保護を通過する必要がある。
- DoD コンポーネントのデータセンターエンクレーブ内の電子メールサーバーから、BCAP 経由で CSO 内のミッションオーナーのエンクレーブ内の L4/5 電子メールサーバーに送信されたすべての電子メール転送は、EEMSG アウトバウンド保護を通過する必要がある。

この要件と TASKORD の解釈は、CSO におけるミッションオーナーの環境が、SaaS のプライマリサービスまたは PaaS/SaaS への補助サービスとして、または IaaS の中でミッションオーナーによってインスタンス化された E メールサーバーを含む DoD エンクレーブと見なされるものという事実に基づいている。

2 人のミッションオーナーが同じ電子メール用の SaaS と電子メールサーバーを利用する場合、異なるミッションオーナーのユーザ間で EEMSG による Eメールの保護は必要とされない。しかし、CSO が異なるミッションオーナーのために異なるサーバー／エンクレーブを実装する場合、CSO には、これらのサーバー／エンクロージャー間の電子メール転送がルーティングされる電子メール保全／保護サービスが含まれていなければならない。この場合、

サーバー間の電子メールトラフィックは、CSP のインフラストラクチャ内留まり、BCAP または EEMSG を通過しない。同様に、IaaS に電子メールサーバーを実装しているか、CSO ベースのエンクレーブ内に PaaS 機能を利用しているミッションオーナーは、SaaS の場合と同様のルールに従い、ミッションオーナーのエンクレーブからミッションオーナーのエンクレーブのトラフィックについて CSO 内で電子メールの保全／保護サービスを提供するか、またはそのようなトラフィックを BCAP と EEMSG を通さなければならない。

すべての BCAP はミッションオーナー用をサポートし、電子メールサーバーを備えたすべての CSO のために、接続の CAP 端で EEMSG 機能との間でサーバー間のトラフィックの適切なルーティングを実装する必要がある。これには、そのようなサーバーとの間のルーティングや、外部とインターネットに接続されている電子メールサーバーの IAP が含まれる。これは CSO の接続承認要件である。しかし、CSO を利用することや、IaaS/PaaS の中でシステム／アプリケーションを実装することは、最終的に TASKORD のコンプライアンスに対するミッションオーナーの責任である。

注：CC SRG のこのリリース時点で、EEMSG は現在、イントラ・エンクレーブ電子メールを検査していない。したがって、上記の要件は、EEMSG がエンクレーブ間の電子メールを検査するまで、CSO の DISN およびミッションオーナーのエンクレーブ内に留まる電子メールトラフィックには適用されない。つまり、EEMSG がインターネットベースの電子メールサーバー間のすべての電子メールトラフィックを検査するための要件は依然として適用される。

第 6 章 サイバー空間防衛とインシデントレスポンス

注意：この版の CC SRG は、DoD Joint 出版物 3-12 (R)「サイバー空間の運用」および DoDI 8530.01「DoD 情報ネットワーク運用へのサイバーセキュリティ活動のサポート」で定義されている新しいサイバー空間防衛用語集と連携している。また、DoDI 8530.01 の発行と DRAFT クラウド CND CONOPS (廃止) を DRAFT DoDM 8530.01「DoDIN の運用および防御的サイバーオペレーションに対するサイバー空間活動のサポート- 内部防護措置 (DCO-IDM)」に置き換えることにより、CSP に適用可能で DoDM 8530.01 から開示可能な内容が以降の版に含まれる。ミッションオーナー等は、DoDM 8530.01 が出版された場合は、それを参照のこと。

サイバー空間防衛は、ネットワークと情報システム (IS:Information Systems) の防衛と保護、脅威の検出、およびインシデントへの対応への取り組みである。サイバー状況認識は、DoD のシステムとデータの使用、保護、防衛に関する共同意思決定の質と適時性を向上させるものである。DoD のサイバー空間防衛活動は、DoDIN を守るための脅威とインシデントに

対応する手段を提供している。このセクションでは、重要なサイバー空間防衛活動；役割と責任；インシデント報告と対処；他のサイバーセキュリティプロセスについて述べる。

6.1 サイバー空間防衛の概要

DoD は、DoDI 8530.01 「DoD 情報ネットワークオペレーションへのサイバーセキュリティ活動のサポート」で定義されているサイバーセキュリティ体制を運用している。この体制は、トップレベルの組織として米国サイバー軍 (USCYBERCOM: United States Cyber Command) と統合軍司令部の DoDIN (JFHQ-DoDIN: Joint Forces Headquarters-DoDIN) 及び DoD のポリシーに従って USCYBERCOM で認定されたサイバーセキュリティサービスプロバイダー (CSSP: Cybersecurity Service Provider) を含むものである。各 DoD の情報システムは、情報システムと関連資産の監視と保護を行う、認定された CSSP と連携したミッションオーナーによって運用／管理される。ミッションオーナーは、SRG/STIG と DoD のポリシーとともに担当の CSSP の支援を受けて、システムのセキュリティ態勢の実装および維持の責任を負っている。CSSP は、DoD ネットワークと情報システム全般のサイバー状況認識を担当している USCYBERCOM へ情報を報告する。USCYBERCOM はまた、さまざまな情報源から収集された脅威情報と脅威の軽減策を CSSP とミッションオーナーに提供している。

注：ミッションオーナーがシステムのセキュリティの態勢を維持する例として、パッチ／アップグレードと IAVM 準拠の適用がある。これは、ミッションオーナーレベルの活動または責任である。一部の DoD コンポーネント（例えば陸軍）は、システムの CSSP（たとえば ARCYBER）へ実行を転移することによって、ミッションオーナーに多少またはすべてのセキュリティ体制の維持活動を軽減させているが、ミッションオーナーレベルの活動と責任はそのまま残っている。したがって、CSSP は、転移されたミッションオーナーレベルの機能を CSSP レベルの機能とともに実行する責任がある。

6.2 クラウドコンピューティングにおける影響レベルのコンセプト変更

商用クラウドコンピューティングへの移行に伴い、DoD はネットワーク防衛機能とプロセスを適用する際に、リスクベースのアプローチを採用している。セクション 3.2 「情報の影響レベル」で説明しているように、DoD は、データのリスクとタイプに見合った情報影響レベルを定義していて、より高いレベルでは保護が強化されている。

影響レベル 2 のデータでは、データの全体的な価値はミッションクリティカルでもセンシティブでもないため、より高い影響レベルのデータと同じレベルの保護を保証することはできないが、保護は必要である。影響レベル 2 のデータは機密性の要件が最小限であることを認識し、責任を持つ A0 が許容できるレベルのセキュリティとリスクを達成するために、

完全性と可用性を重視する必要がある。情報システムへのユーザ接続は、CSP のインターネット接続を介して行われるため、DoD は CS0（利用できる場合）を通じて利用可能なネットワーク境界保護と監視に頼っている。境界防御が CSP によって実装されていない場合、ミッションオーナーが責任を持って DoD の CSSP と調整する必要がある。システム／ホスト／アプリケーションのレベルでミッションシステムをサポートする保護機能は、CSSP とミッションシステム管理者（SaaS の CSP を含む）の組み合わせによって提供される。IaaS/PaaS を使用した関連する境界条件については、セクション 5.10.6「IaaS/PaaS を利用したミッションオーナーのシステム／アプリケーション要件」を参照のこと。CSP は、適切な境界保護と CSSP サービスを適用することによって、SaaS CS0（およびミッションオーナーが支配権を持たない PaaS CS0）を保護することが期待されている。すべてのサービスモデル I/P/ SaaS に関する追加情報および CSP 要件については、5.10.3「CSP サービスのアーキテクチャ」とサブセクションを参照のこと。

レベル 4 以上のデータについてはリスクが高いことから、強力な監視、イベント相関、分析を可能にするエンタープライズ防衛の仕組みとデータ収集が必要である。レベル 4 以上のデータの DISN 境界は、DoD CAP と DoD ミッションをサポートする CSP のネットワークインフラストラクチャとの間の接続を通じて本質的に拡張される。したがって、イベントはいくつかの異なるエンティティ；CS0（特に SaaS の）の監視による CSP；ミッション管理者または所有者またはミッションと境界接続の監視をサポートしている CSSP によって検出される可能性がある。インシデントを迅速に調査し、対応するためには、すべてのエンティティが協力して作業する必要がある。DoD BCAP の保護は、境界サイバー空間アクションを実行する組織によってサポートされている。

6.2.1 境界サイバー空間防衛アクション

境界サイバー空間防衛（BCD:Boundary Cyberspace Defense）アクションは、認可された BCAP を介して CSP との間の接続を監視して防御を行う。BCD アクションは、個々の BCAP を流れるすべての接続のクロス CSP 分析とともに、各 CSP 相互接続が個別に DoDIN に対面するリスクを防ぐ。これらのアクションは特定の BCAP による接続に焦点を当てているが、脅威が単一の CSP または BCAP を超えているかどうかを判断するには、クロス BCA 分析が必要である。

6.2.2 ミッションサイバー空間防衛アクション

ミッションサイバー空間防衛（MCD:Mission Cyberspace Defense）アクションは、ミッションオーナーのクラウドベースのミッションシステム／アプリケーションと仮想ネットワークにサービスを提供している。MCD アクションを実行する組織は、複数の CSP と複数の CS0 でインスタンス化された、クラウドベースのミッションシステム／アプリケーションと

仮想ネットワークにサービスを提供できる。MCD アクションは、クラウドコンピューティングの要素に焦点を当て、認定された DoD CSSP によって実行される。MCD アクションは、典型的には、クラウドベースでない IS のためにミッションオーナーのコンポーネントによって使用される CSSP によって実行される。ただし、ミッションオーナーは、MCD アクションを実行するために、認定された任意の CSSP へ資金を提供して利用することを選択できる。

6.3 サイバー空間防衛アクション

以下は、サイバー空間の防衛アクションとクラウドオペレーションと関連したアクションのリストである。

- **DoDIN サイバー空間防衛 (DCD:DoDIN Cyberspace Defense) アクション** : DCD アクションを実行する組織の主な目的は、DODIN 全体の攻撃に対する連携した対処の統制である。DCD は、ミッションオーナー、MCDs、BCDs、CSOs、および CSP の間で、運用環境の幅広いイメージを構築している。DCD は、インシデントやイベントのパターンを特定し、関連するインシデントチケットを統合し、軽減策を指示し、DODIN サイバープロテクションチーム (CPT: Cyber Protection Teams) を割り当てて、特定の脅威や敵に努力を集中させる。具体的なサイバー空間防衛アクションには ;
 - イベント／データのクロス BCAP 相関と分析を通じて、商用クラウドインフラストラクチャの DoDIN と DoD ミッションシステムを保護する。
 - BCAP または CSP を含む DoDIN 全体のインシデントとシステムに関する状態の報告について、サイバーセキュリティの対処の指示または推奨を行う。
 - DoDIN 全体の事案について、CSP と外部コミュニケーションを確立・維持し、MCD と BCD を含むすべてのエンティティ間で DoD 内のコミュニケーションを確立する。
 - 関連する CSP の情報を入手するための US-CERT とのインターフェース ; BCD/MCD アクションを実行しているすべての組織間での情報の相互共有を確実にする。
- **境界サイバー空間防衛 (BCD:Boundary Cyberspace Defense) アクション** : BCD アクションを実行する組織の主な目的は、許可された CSP が境界クラウドアクセスポイント (BCAP: Boundary Cloud Access Point) 経由の専用接続を介し、DISN へ影響を及ぼすパブリック、プライベート、ハイブリッド、またはコミュニティクラウドを利用するイベントやインシデントから防衛情報システムネットワーク (DISN) を保護することである。BCD アクションは、クラウドでホストされているシステム、アプリケーション、およびデータを守る目的で MCD のサポートを行う。具体的なサイバー空間防衛アクション

ンは；

- BCAP 経由で DISN を保護する。
- MCD アクションを実行する組織に関連する BCD が収集した兆候および警告へのタイムリーなアクセスを提供する。
- DCD アクションをサポートして、複数のミッションオーナー、CSO、または CSP に影響を与える関連イベントまたはインシデント間の相関関係を特定する。

- **ミッションサイバー空間防衛 (MCD) アクション：**MCD アクションを実行する組織の主な目的は、ミッションオーナーのシステム、アプリケーション、およびクラウドでホストされているデータの防御である。MCD アクションは、有機的な組織とサブスクリバの代わりにサイバーセキュリティサービスプロバイダ (CSSP) によって実行される。具体的なサイバー空間防衛アクションは；

- ミッションオーナーのサイバーインシデントやイベントの分析
- CSP の IaaS/PaaS インフラストラクチャの中のミッションオーナーのクラウドベースのシステム、アプリケーション、および仮想ネットワークの監視、保護、防御
- CSO の中のミッションオーナーのクラウドベースのデータの監視、保護、防御
- BCAP、仮想プライベートネットワーク (VPN)、インターネットアクセスポイント (IAP)、パブリックサーバーへの直接インターネットアクセス、またはその他を介した CSO へのすべての接続の防護
- 特権のアクション (例えばクラウドの管理やミッションオーナーのアプリケーション運営) およびミッションオーナーのアプリケーションに対するイベントやインシデントの監視 (例えば、SQL インジェクション)
- 複数のミッションオーナー、CSO、または CSP に影響を及ぼす関連イベントまたはインシデント間の相関を特定する DCD の取り組みのサポート
- ミッションオーナーを含むすべてのエンティティと、MCD および BCD アクションを実行する組織との間での、DoD 内部のコミュニケーションの確立

6.4 サイバー空間防衛の役割と責任

以下は、クラウドオペレーションに関連するサイバー空間防衛の任務と責任のリストである。

- **JFHQ-DoDIN：**JFHQ-DoDIN は DCD アクションを実行し、DoD コンポーネントに対して直接のタスク権限を持つ。JFHQ-DoDIN は、USCYBERCOM の一環として、米国 Computer Emergency Readiness Team (US-CERT) など、DoD 以外の組織と協力する法的権限を持

っている。

- **DoD のコンポーネント**：サービスサイバーコンポーネント、国防機関、および DISA は、ミッションオーナーを支援するために MCD アクションを実行することができ、BCD アクションは、BCAP の運用、監視、および保守の責任を負う際に実行される。
- **ミッション管理者**：ミッションオーナーのクラウドベースのシステム、アプリケーション、および仮想ネットワークの管理者で次の責任を持つ；
 - ミッションオーナーからの指示と命令に従う
 - クラウドベースのミッションシステム、アプリケーション、および仮想ネットワークの維持およびパッチ適用
 - クラウドベースのミッションシステム、アプリケーション、および仮想ネットワークの保護対策のインストールと維持

注：セクション 6.1 「サイバー空間防衛の概要」で述べたように、一部の DoD のコンポーネントは、MCD アクションを実行する組織にこれらの責任の一部または全部を移転する可能性がある。

- **クラウドサービスプロバイダ (CSP)**：CSP は、顧客 (DoD のミッションオーナー) のシステム、アプリケーション、および仮想ネットワークのためのセキュアな環境を提供するために、独自のサイバー空間防衛サービスを提供している。実際には、CSP はミッションオーナーの延長として機能している。最低限、CSP は以下の責任を負う；
 - インフラストラクチャとサービス提供の範囲内で、サイバー空間防衛の現地における運用指導とサポートの提供
 - すべてのサービス提供をサポートするインフラストラクチャ、オペレーティングシステム、およびアプリケーションの完全な維持、パッチ適用、監視、保護
 - サービス提供の SLA/説明やミッションオーナーの SLA/契約で定められている、責任を負う (無しから全部まで変化) OS とアプリケーションを提供する PaaS サービスの一部の完全な維持、修正、監視と保護
 - DoD のデータ／情報を含む OS とアプリケーションを提供する SaaS サービスの完全な維持、パッチ適用、監視、保護
 - 契約している場合：
 - ・ DoD クラウドベースミッションシステム／アプリケーションとデータに対する脅威のインシデントレスポンスと脅威軽減に関する MCD アクションを実行する組織との調整
 - ・ タイムリーなインシデントとシステムのヘルスレポートの提供
 - 双方向のサイバー状況認識の維持

- **ミッションオーナー**: 全体的な任務環境に対して責任がある個人/組織は、システムの機能とサイバー空間防衛の条件が満たされていることを確保する。CSP の CS0 加入者であるミッションオーナーは、CSP と契約上の関係にある。ミッションオーナーは、サービスレベル合意書 (SLA: Service Level Agreements) にそのような文言を含めることによって、MCD と BCD アクションを実行している組織に、サイバー空間防衛関連のレポートをオプションで展開することができる。少なくとも、ミッションオーナーは次の責任を負う:
 - 任意の CSP の IaaS/PaaS インフラストラクチャ (DoD が商用/非 DoD エンティティによって運営されているか運営されているかにかかわらず) におけるミッションオーナーのシステム、アプリケーション、および仮想ネットワークの防御を提供する MCD アクションを実行する組織のサービスに関与し、資金を提供すること。
 - インシデント報告、インシデントレスポンス、MCD および BCD アクションを実行する適切な組織との連絡のための、CSP との契約における条件と要求事項の設定

6.5 サイバーインシデントの報告と対応

このセクションに関連する CNSSI 4009、IA 用語集に反映されている 2 つの重要な定義は次のとおりである。

サイバーインシデント (cyber incident) :

情報システムやそこに存在する情報に実際または潜在的に悪影響をもたらすコンピュータネットワークの使用によって行われるアクション。インシデントを参照。

インシデント :

情報システムの機密性、完全性、可用性 ; またはシステムが処理、保管、送信する情報、またはセキュリティポリシー、セキュリティ手順、許容される利用ポリシーに対する違反や差し迫った脅威など、実際または潜在的に危険にさらすと評価された事案。

この SRG では、インシデントとサイバーインシデントを同じ意味で使用している。

FedRAMP は、IR-6 の選定と実施を通じて、CSP にサイバーインシデントを国土安全保障省 (DHS) の米国コンピュータ緊急準備チーム [US-CERT]¹⁰⁴ と情報を利用する連邦政府機関に報

¹⁰⁴ US-CERT: <https://www.us-cert.gov/>

告することを要求している。DoD（影響レベル 2～5）以外の連邦政府機関間で共有または多重共有されている CSO の場合、FedRAMP の要求に応じて DoD への報告と並行して US-CERT にインシデントが報告される。DoD（影響レベル 4 以上）に専用のインフラストラクチャを提供する CSP の場合、そのインフラストラクチャと CSO に関するインシデントは US-CERT に報告されるのではなく、直接 DoD へ報告される。USCYBERCOM/JFHQ-DoDIN は US-CERT および必要に応じて他のエンティティとの調整を行う。DoD のインシデント報告プロセスは、セクション 6.5.3 「インシデント報告のメカニズム」で説明されている。

DoD ミッションを積極的にサポートしている CSP は、MCD アクションを実行する 1 つ以上の組織からサポートされている。MCD アクションを実行する組織は、CSP の運営組織が CSP のセキュリティ体制や CSP のクラウドサービスの提供に影響を与えるインシデントへの対応を調整する DoD の連絡先となる。MCD アクションを実行する組織は、必要に応じて BCD アクションを実行している組織と連携する。

対応するセキュリティ管理策：IR-4、IR-5、IR-6

6.5.1 インシデントレスポンス計画と補遺

CSP は、DoD のサイバー空間防衛の統括要件を満たすためのアプローチを、インシデントレスポンス計画の一部またはインシデントレスポンス計画補遺の一部として提供している。CSP は、その PA または DoD クラウドサービスカタログに含める条件として、審査と承認のため、DISA で利用可能な計画や補遺を作成する。CSP は、FedRAMP が選択したセキュリティ管理策 IR-1 の要求に応じて、インシデントレスポンス計画の更新および送付と併せてインシデントレスポンス計画補遺（使用されている場合）を更新し提供する。CSP は特にサイバーインシデントやデータ侵害に対処する必要がある、このサイバーインシデントには、制御の喪失、侵害、許可されない目的で電子的や非電子的形式による政府データの取得、アクセスなどが含まれる。CSP は、計画やその補遺に、インシデントの日時場所にかかわらず、すべてのインシデントに対処し、データの違反について政府に通知するようにしなければならない。計画または補遺には、インシデントの発生時に、政府が遵守を要求している以下の（これに限定されない）ポリシーや手続きを組み込む必要がある。

- セクション 6.5.3 「インシデント報告メカニズム」で規定されたインシデント報告プロセスに従った、インシデントを政府へ報告
- このような措置を取るための、期間を含むインシデントの軽減や救済するための特定の手順（例えば、個人識別情報（PII:Personally Identifiable Information）データ漏えいについては 1 時間以内の報告、一般的に流出と呼ばれる格付け情報の不注意な開示(NDCI:Negligent Disclosure of Classified Information))

- どのような状況下や方法で、インシデントの影響を受けた個人または団体について、誰から通知されるか；そして
- 米国政府のデータに影響を与える、または影響を及ぼす可能性のあるコンピュータセキュリティインシデントを処理するためのその他の特別な指示で、DoD、NIST、US-CERT、および CNSS がインシデント管理、分類、修復のために発行したガイダンスおよびポリシーの指示に沿ったものであること；またはその他の適用可能な法、規制、指示、または方針に従うこと。

対応するセキュリティ管理策：IR-8

6.5.2 情報要件、カテゴリ、タイムライン、およびフォーマット

DoD のミッションとシステムを守ることは、すべての組織（CSP、MCD または BCD アクションを実行する組織、ミッションオーナーとミッション管理者）がチームとして協力して作業を行うことが共通の責任である。イベントは、接続のアーキテクチャ（直接インターネットか、または CAP を介してか）に応じて、次のエンティティのいずれかによって検出される可能性がある。

- CSO の監視（特に PaaS/SaaS の場合）を通じた CSP の要員
- ミッション管理者またはオーナー（PaaS/SaaS の CSP を含む）
- モニタリングを通じた MCD アクションの実行を支援する組織
- BCAP の監視を通じた BCD アクションの実行を支援する組織

イベントやインシデントをすばやく調査して対応するには、すべてのエンティティが協力して作業する必要がある。CSP がその環境でサイバー空間防衛を実行する過程で、権限のない人物が政府データにアクセスする可能性がある状況に焦点を当てて、CSP は情報システムを監視し MCD アクションを実行する組織に関連情報の報告を行う。

DoD に対する CSP の報告要件は、より幅広い連邦政府の報告要件のために US-CERT が使用する報告用語と同じである。インシデント通知には、インシデントの説明とできるだけ多くの以下の情報が含まれている必要がある。

- 契約番号、USG 契約担当者の連絡先情報、契約のクリアランスレベルなどを含む契約情報
- 影響を受けた組織と報告組織ならびに MCD の連絡先情報
- 関連する脆弱性（CVE：Common Vulnerabilities and Exposures）識別子など
- タイムゾーンを含む発生日時
- 検知と識別の期日／時間（タイムゾーンを含む）

- 関連インジケータ（ホスト名、ドメイン名、ネットワークトラフィック特性、レジストリキー、X.509 証明書、MD5 ファイル署名など）
- 既知の場合は脅威ベクトル（US-CERT 連邦インシデント通報ガイドラインの脅威ベクトル分類と原因分析フローチャートを参照）
- 優先順位付けの要素（すなわち、米国 CERT 連邦インシデント通報ガイドライン¹⁰⁵内の定義されたフローチャートによる機能的影響、情報への影響、および回復可能性）
- 送信元および宛先インターネットプロトコル（IP）アドレス、ポート、およびプロトコル
- 影響を受けるオペレーティングシステム
- 軽減要因（全ディスク暗号化または 2 要素認証など）
- 可能な場合、実行した対処
- システム機能（Web サーバー、ドメインコントローラ、またはワークステーションなど）
- 物理的なシステムの場所（例：Washington DC、Los Angeles、CA）
- インシデントの識別に使用された情報源、方法、ツール（侵入検知システムや監査ログ分析など）
- インシデントに関連した、上記に含まれていない追加情報

最初のインシデントレポートは、発見から 1 時間以内に提出され、追加の情報は都度提供される。CSP と MCD/BCD アクションを実行する組織間の、コミュニケーションとチームワークに活かすには、最初のレポートが不完全な場合がある。CSP は、タイムリーな報告（重要な情報を含む不完全な報告）と完全な報告（すべてのブロックが完了した報告）のバランスをとるべきである。タイムリーな報告が不可欠であり、詳細が判明すれば完全な情報として追加すべきである。

注：これらの要件は、すべての情報影響レベルで、すべてのシステムに適用される。CSP は、サイバー空間防衛アクションを行う DoD 組織と連携する際に、これらの要件に従わなければならない。ミッションオーナーは、レベル 2 の場合でも、これらの要件を契約に含める必要がある。

対応するセキュリティ管理：IR-5、IR-6、IR-8

¹⁰⁵ US-CERT Federal Incident Notification Guidelines: https://www.uscert.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf

6.5.3 インシデント報告メカニズム

DoD CSP (例: milCloud's) のサイバー空間防衛プロバイダは、通常の DoD プロセスに従って、共同インシデント管理システム (JIMS: Joint Incident Management System) を使用してすべてのインシデントの報告を行う。

DFARS Clause 252.204-7012 (d) が、クラウドコンピューティングのために更新されて確定されたとき、次の要件と整合。

レベル 2/4/5 の商用 CSP は、オンライン防衛産業基地 (DIB: Defense Industrial Base) のサイバーインシデント収集フォーマット (ICF: Cyber Incident Collection Format) ¹⁰⁶ を通じて、すべてのインシデントの報告を行う。オンライン形式の使用が望ましい。この形式へのアクセスには、DoD が承認した中度 (medium) な保証の外部認証局 (ECA: External Certificate Authority) 証明書が必要である。この形式にアクセスできない場合は、電話 (877) 838-2174 または電子メール: DCISE@DC3.mil まで連絡のこと。

CSP は、ルーティング目的のために、インシデントの影響を受けるすべての DoD ミッションに対して MCD アクションを実行する組織の連絡先 (POC: points of contact) をすべて含める必要がある。これは、契約管理者などヘルパーティングするためにツールが必要とする他の POC に加えてある。MCD アクションを実行する組織は、レポートを受け取ると、JIMS を介して DoD の報告プロセスを開始する。

格付けされたインシデント報告が適切で指示されている場合、CSP は SIPRNet 電子メールまたは安全な電話/ファックスを使用して、指定されたインシデントを報告および調整を行う。レベル 6 の商用 CSP は、SIPRNet 電子メールまたは、セキュアな電話/ファックスを利用して、MCD アクションを実行する組織へすべてのインシデントを報告し、指定されたインシデントの報告と調整を行う。

情報の機密性と完全性についてリストされた暗号化されたメカニズムと同等のレベルの保証を示すことができれば、サイバー空間防衛情報のいくつかまたはすべてのクラスについて、CSP とその顧客との間で既に通信している CSP の既存の通知メカニズムを使用することができる。

対応するセキュリティ管理策: IR-6、IR-8

¹⁰⁶ DIBNet CS/IA Portal: <http://dibnet.dod.mil/>

6.5.4 クラウドにおけるデジタルフォレンジックと法執行／犯罪捜査のサポート

インシデントや侵害は発生するものである。その場合には、報告され、法的に分析されて、将来どのようにシステムを保護して防止するのか、潜在的に誰に責任があるのかに関する詳細な情報を得る必要がある。インシデント情報は、必要に応じて法的な訴追をサポートする方法で収集し、処理する必要がある。このように、収集されてから必要がなくなるまで、改変から保護する必要がある。フォレンジックのサポートは、ミッションオーナーと CSP の間で、サービスの種類に応じてさまざまなレベルで共有される。

クラウド内のデジタルフォレンジックには、NIST の標準技術協会または内部報告書 (NISTIR) 8006「クラウドコンピューティング・フォレンジックサイエンスチャレンジ」のドラフトに記載されているように、多くの課題がある¹⁰⁷。CC SRG のこのセクションでは、クラウドフォレンジックを可能にして実行し、法執行および刑事捜査 (LE/CE:Law Enforcement and Criminal Investigation) 活動を支援する。次の要件は、すべての情報影響レベル 2～6 に適用される。

対応するセキュリティ管理：IR-4、IR-5 (1)

6.5.4.1 悪意のあるソフトウェア

報告されたサイバーインシデントに関連した、悪意のあるソフトウェアを発見し隔離する CSP またはその下請け業者は、CSP によって採用されている他の分析機関に加えて、MCD アクションを実行する組織へ、悪意のあるソフトウェアを安全に提出するものとしている。提出手段は、MCD アクションを実行する組織と調整を行う。DoD サイバー空間防衛コミュニティは、DoD ネットワークとミッションオーナーのシステムに適用される検出シグネチャと緩和策を開発するために分析結果を活用する。分析結果は、許可されて適切な通信チャネルが存在する場合、CSP と共有される。

対応するセキュリティ管理策：SI-3 (10)

6.5.4.2 インシデント情報の収集、保存、および保護

SaaS を含むすべてのサービスタイプの下で、CSP がインフラストラクチャや CSO 内で発生したサイバーインシデントを発見した場合、CSP はインシデントの初期報告とともに、CSO と顧客をサポートしている影響を受けたシステム／サーバー／ワークステーションのイメージとステートを収集、保存、保護する責任がある。これには、システムログ、揮発性メモリのキャプチャ、ハードドライブ（物理または仮想）イメージが含まれる。また、CSP は関

¹⁰⁷ NISTIR 8006: <http://csrc.nist.gov/publications/PubsDrafts.html>

連するすべてのネットワークログだけでなく、利用可能なすべてのネットワーク監視／パケットキャプチャ・データを保存し、保護するものとする。この情報は、発見後できるだけ早く収集されなければならない。

CSP は、所要のサイバーインシデントレポートの提出から少なくとも 90 日間、捕捉されたインシデント情報を保持し、DoD からの情報要求や関心の低下に対応する必要がある。この要件は、IaaS、PaaS、SaaS をサポートする基盤となるインフラストラクチャ、PaaS の下で CSP によって管理されるシステムとアプリケーション、SaaS のすべてのシステムとアプリケーションに適用される。

IaaS の下で、ミッションオーナーがシステム／アプリケーション／仮想ネットワーク内でサイバーインシデントが発生したことを発見すると、MCD アクションを実行する組織と一緒に行動し、それらの仮想ネットワークで発生したネットワークログ、ネットワーク監視／パケットのキャプチャデータを含め、判明した影響を受けるすべての仮想マシンのイメージと状態をキャプチャ、保護、保護を行う。

これには、システムログ、揮発性メモリのキャプチャ、および仮想ハードドライブイメージが含まれる。一般に、侵害された VM の仮想ハードドライブイメージは、サービスされるときに新しいイメージとして保存するのは簡単であるが、侵入された VM をシャットダウンする前に、システムログや揮発性メモリをキャプチャするツールを実行するには詳細な手順に従う必要がある。その一例として、Windows および UNIX/Linux ベースのシステムで必要なサポート情報を収集するためのソフトウェアツールを提供する DISA インシデント対処と復旧チーム (IRRT: Incident Response and Recovery Team) の First Responder's Guide および Web ページ¹⁰⁸ ページが存在する。これらのツールは、VM 内で動作し、VM に割り当てられた揮発性メモリで動作する。他の顧客の情報や、同じ物理ハードウェア上で動作している他のツールに対して、懸念される可能性のある VM を侵害することはない。MCD アクションを実行する各組織は、同様の手順とツールを持っていなければならない。ミッションオーナーや MCD アクションを実行する組織は、その後 CSP と調整して、インシデントの調査をサポートするために関連するインフラストラクチャのログを収集する必要がある。あるいは、CSP は、自分の環境で動作する類似のツール／機能を提供することもできる。

PaaS と SaaS では、ミッションオーナー、MCD アクションを実行する組織、または CSP がインシデントを検出する可能性がある。各当事者は、管理しているサービスの分野に応じて、

¹⁰⁸ DISA IRRT Web site: https://blogs.intelink.gov/blogs/_disairrt (CAC/PIV PKI required)

必要なフォレンジック情報を収集するために他者と協力しなければならない。ミッションオーナーが上記の IaaS で説明したツールを実行することは難しいかもしれないが、CSP は自分の環境で動作する同様のツール／機能を提供する必要がある。

PaaS の下で、ミッションオーナーが契約されたサーバー (VM など) の OS とプラットフォームアプリケーションを管理している場合、IaaS で説明したように、自身や CSP から提供されたツールを使って MCD アクションを実行する組織と連携してキャプチャ、保存し、機能の保護を行うのはそれぞれの責任である。一方、CSP が CSO のサーバー、OS やプラットフォームアプリケーションを管理する場合は、CSP がキャプチャ、保存、および保護機能を実行する必要がある。そして CSP は、その結果をミッションオーナーの MCD アクションを実行する組織と共有する。

SaaS の下では、CSP は CSSP と一緒にキャプチャ、保存、保護処置を実行する必要がある。CSP は、その結果をミッションオーナーの MCD アクションを実行する組織と共有する。

捕捉されたインシデント情報はすべてデジタル証拠である。すべてのデジタル証拠は、システムからコピー／キャプチャされたときに、元の情報とコピーされた情報をハッシュし、最初と将来に、コピーの完全性を検証する必要がある。

効率的に実行するには、すべてのインシデントキャプチャは IR-5 (1) に従って自動化して実行される必要がある。CSP は、インシデントの取得と保護をサポートする、自動化された機能を提供する必要がある、インフラストラクチャ内と顧客の CSO 環境内でのインシデントの調査をサポートする必要がある。CSO 内の環境で、必要に応じて顧客のインシデントレスポンス活動をサポートするために、その機能に対するインターフェースを顧客に提供する必要がある。このようなすべての自動化では、非 DoD または非連邦情報がインシデントレスポンスチームまたはフォレンジック／LE (訳注 Low Enforcement) 調査官に明らかにされないように、顧客が捕捉した情報を分離する方法で情報を取得する必要がある。同様に、政府環境に関連する情報は、CSP の基盤となるインフラストラクチャから取得された情報から分離されなければならない。情報が取り込まれたら、自動化はデータの変更を検出できるようにデータの 1 つ以上のハッシュを作成する必要がある。自動化は、データの機密性と完全性を保つためにデータを暗号化する必要がある。CSP の基盤となるインフラストラクチャからキャプチャされた情報は、政府の環境からキャプチャされた情報とは別に暗号化される。暗号化キーは、フォレンジック分析者に提供され、政府のみが政府の環境から取得した情報の鍵にアクセスできるように格納され、CSP は CSP の基盤となるインフラストラクチャから取得されたデータにアクセスする。

注：現時点では、DISA IRRT ウェブサイト（特に Oscar）に提供されているツールの一部にはライセンスソフトウェアが組み込まれており、DISA IRRT の指示以外の他の組織では使用できない。

ミッションオーナーは、CSP とミッションオーナー/MCD の間の具体的な責任を明確にした契約書/SLA にこれらの要件を反映しなければならない。

対応するセキュリティ管理：IR-4、IR-5（1）、IR-8、SI-12

6.5.4.3 LE/CI のためのフォレンジック／インシデント情報保管の継続性(chain-of custody)

NISTIR 8006 によると、保管の継続性は、証拠の取扱いの時系列的な文書として法的な文脈で定義されており、証拠の改ざんまたは不正行為の主張を避けるために必要である。CSP やミッションオーナーによって発見されたインシデントが、個人によって悪意を持って発生した場合、責任を持つ個人や組織を法的に非難または訴追するためには、情報の管理を維持することが不可欠である。

LE/CI 調査を支援するために、捕捉されたデータの保管の継続性は、インシデントの調査が開始されたときから、エンドツーエンド、人物対人物で文書化する必要がある。情報の各部分または部分をキャプチャする個人は、この文書化を開始し、それを含む情報またはメディアを後で処理する各個人は、その文書化を続行する必要がある。保管の継続性フォームは、上記の DISA IRRT ウェブサイトまたは法執行機関から入手できる。保管の継続性の文書化は重要で推奨されているが、保管の継続性の形式と手順の開始は、事件が法執行の通知を必要とする場合にのみ必要となる場合がある。その場合、連鎖の形式は法執行官によって開始される。要請または召喚された場合、CSP は、CSP の保管の継続性とフォレンジック・データ収集／収集方法に関する宣誓書または専門家の証言を通じて、従業員による証拠の提供を可能にする。

対応するセキュリティ管理策：SI-12

6.5.4.4 CSP による PA 取得に向けたデジタルフォレンジックサポート

CSP は、CSP に関する上記要件をサポートする能力と、特にシステムイメージと状態保存の分野でミッションオーナーに必要な要件をサポートする能力について評価される。これには、ミッションオーナーや CSP によるシステムログ、揮発性メモリキャプチャ、ハードドライブ（物理または仮想）イメージのキャプチャと保存をサポートする機能とツールが含まれる。CSP は、セキュリティ計画でデジタルフォレンジックをサポートする能力を文書化する。

る必要がある。CSP のフォレンジックサポート機能とその受入れ可能性は、PA をサポートする情報に文書化される。

6.6 警告、戦術的な指示と命令

USCYBERCOM または JFHQ-DoDIN は、BCD と MCD アクションを実施する組織に警告、戦術的な指示、および命令を伝える。BCD と MCD アクションを実行する組織は、個々の CSP への適用可能性を分析し、USCYBERCOM または JFHQ-DoDIN および CSP と適切に連絡をとりあう。CSP は、指示と対策を実現するために、MCD アクションを実行する組織やミッションオーナーと連携する。

CSP は、FedRAMP が選択したセキュリティ管理策 SI-5 の要求に従って、ミッションオーナーに代わって、MCD アクションを実行する組織から発せられた通知や指示を受けて対処・行動し、報告することができなければならない。

6.7 継続的モニタリング／行動計画とマイルストーン (POA&Ms)

企業内の既存の脆弱性とリスクを理解することは、効果的なサイバー空間防衛の分析を実行する上で重要な要素である。FedRAMP と FedRAMP+の両方の要件をサポートする継続的な監視要件の一部として、CSP によって開発された脆弱性レポートと POA&Ms (Plans of Action and Milestones) は、DISA のクラウドサービスサポートチームと、その後、サイバー空間防衛を提供するために MCD と BCD アクションを実行する組織に提供される。

発見した高およびクリティカルなリスクについては、FedRAMP と FedRAMP+の両方の要件により、30 日以内に低減する必要がある。中程度については、90 日以内に低減する必要がある。

対応するセキュリティ制御：CA-5、CA-7

6.8 計画停止の通知

ミッションシステムに影響を及ぼす計画された停止は、ミッションオーナーによって調整される。運用コミュニティへの影響を最小限に抑えることを目標としている。承認された停止は、許可されたサービス中断 (ASI: Authorized Services Interruption) と呼ばれる。CSP は、サービスの停止発生時とサービスの復帰時に、管理下にある ASI の MCD アクションを実行しているすべての影響を受ける組織に通知する必要がある。複数のミッション環境に影響を及ぼす停止または変更は、より広い状況認識を可能にするために、BCD アクションを実行する組織により、MCD アクションを実行する組織へ報告されなければならない。ミッ

ションオーナーと管理者は、ASI が管理下にあるときに MCD アクションを実行する組織に対して同じ通知を行う責任がある。

6.9 サイバー空間防衛のための PKI

DoD PKI プログラムは個人の身元の保証を提供し、これは、C2 やサイバー空間防衛に関する情報の共有において重要である。このセクションでは、DoD サイバー空間防衛担当者と安全に通信する CSP 要員の信頼できる身元を確立するための要件を概説している。セクション 6.5.3 「インシデント報告メカニズム」に示された手順を経てインシデントが報告され、署名または暗号化された電子メールが後続の通信方法として使用される場合、DoD PKI 証明書が次のように必要とされる。

影響レベル 2～5：CSP は、好ましくは暗号化された電子メールを介して DoD と通信する必要がある各人に対して、DoD PKI 証明書または DoD 認定の PKI 証明書のいずれかを持っていなければならない。DoD で承認された資格情報の詳細については、IASE PKI /ECA Web ページ¹⁰⁹および PKI/PK Enabling (PKE) Web ページ¹¹⁰を参照。同等の代替手段は、ケースバイケースで評価される。

影響レベル 6：レベル 6 のシステムを提供する CSP は、SIPRNet への接続により、システム管理者用の SIPRNet トークン/NSS PKI 証明書を既に取得している。インシデントレスポンスとサイバー空間防衛の担当は、暗号化された電子メールを介して DoD と通信するために SIPRNet トークン／証明書を使用する。

6.10 脆弱性と脅威情報の共有

脆弱性と脅威情報の共有は、DoD がサービス提供中に収容または処理された DoD 情報を保護し、防御するために、DoD にとって非常に効果的な方法である。US-CERT や USCYBERCOM などの政府機関は、詳細な脆弱性情報を提供している。いくつかの商用ソースは、インフラストラクチャをさらに守るために CSP によって使用される補足的な情報も提供している。CSP は、そのような知識ソースを活用することが奨励されている。しかしながら、DoD が CSP に提供できる情報の多くは、格付けされている。そのような情報を得る手段は以下の通りである：

¹⁰⁹ IASE PKI/ECA page: <http://iase.disa.mil/pki/eca/Pages/index.aspx>

¹¹⁰ IASE PKI/PKE Page: <http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx>

防衛産業基盤サイバーセキュリティ／情報保証プログラム¹¹¹（DIB CS/IA:Defense Industrial Base Cybersecurity/Information Assurance Program）は、DIB 格付けなしの情報システム上に存在または通過する DoD 情報を保護するために、DIB 参加者の能力を強化し補完するプログラムである。この自発的な官民のサイバーセキュリティパートナーシップの下で、DoD と参加する DIB 企業は、非格付けと格付けされたサイバー脅威情報、ベストプラクティスおよび緩和戦略を共有している。サイバーインシデントレポートはこのパートナーシップの成功に重要な要素であるが、プログラムの真価は DoD 情報をより安全にするために重要なコラボレーションである。DIB CS/IA のメンバーシップにより、DIB 参加者は、データ共有とコラボレーションに使用される非格付けと格付けされたネットワークである DIBNet-U と DIBNetS へのアクセス権を取得することができる。DIBNet へのアクセスにより、CSP は CYBERCOM の通知、格付けされた電子メール、および DIB Web ポータルへのアクセスを提供している。

DIBNet へのアクセスは、CSP に、非格付けと格付けされたサイバー脅威情報（緩和戦略を含む）の両方へのアクセスを提供する。DIB CS/IA プログラムのメンバーシップは任意であるが、セクション 6.5.3 「インシデント報告メカニズム」に記載されているサイバーインシデント報告は必須である。適格な CSP は、より高い価値の DoD データおよびシステムをホストするインフラストラクチャの保護を促進するために、DIB CS/IA プログラムに参加することが推奨されている。

注：DoD CSP は既にサイバー空間防衛通信アーキテクチャに統合されており、確立されたチャンネルを介して非格付けの CYBERCOM の通知を受信する。

¹¹¹ DIBNet CS/IA Portal: <http://dibnet.dod.mil/staticweb/index.html>

付録 A 参考文献

1. Public Law 93-579, as codified at 5 U.S.C. 552a, Privacy Act of 1974
<http://www.archives.gov/about/laws/privacy-act-1974.html>
2. Public Law 104-191, Health Insurance Portability and Accountability (HIPAA) Act of 1996 <http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html>
3. Public Law 83-703, Atomic Energy Act of 1954, as amended,
<http://pbadupws.nrc.gov/docs/ML1327/ML13274A489.pdf#page=23>
4. 22 Code of Federal Regulations (CFR), 22 CFR 120.15 - US Persons, 120-16 - Foreign persons, <https://www.gpo.gov/fdsys/pkg/CFR-2011-title22-vol1/pdf/CFR-2011-title22-vol1-sec12015.pdf>
5. 22 Code of Federal Regulations (CFR), 22 CFR 120.17 - Export,
<https://www.gpo.gov/fdsys/pkg/CFR-2004-title22-vol1/pdf/CFR-2004-title22-vol1-sec12017.pdf>
6. 22 Code of Federal Regulations (CFR), 22 CFR 120.-130 International Traffic in Arms Regulations Part 123 - Licenses for the Export of Defense Articles,
https://www.pmddtc.state.gov/regulations_laws/itar.html
7. 8 U.S. Code § 1408 - Nationals but not citizens of the United States at birth, <https://www.gpo.gov/fdsys/pkg/USCODE-2010-title8/pdf/USCODE-2010-title8-chap12subchapIII-partI-sec1408.pdf>
8. Executive Order 13526: Classified National Security Information, dated 29 December 2009. <http://www.archives.gov/isoo/policy-documents/cnsi-eo.html>
9. Executive Order 12829 - National Industrial Security Program, January 1993.
<http://www.archives.gov/isoo/policy-documents/eo-12829.html>
10. Executive Order 13556 - Controlled Unclassified Information.
<https://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlledunclassified-information>
11. EO 12958, Classified National Security Information (April 17, 1995) as amended by EO 13292. <http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html>
12. 48 Code of Federal Regulations (CFR) Subpart 4.4 - Safeguarding Classified Information within Industry. <https://www.gpo.gov/fdsys/granule/CFR-2011-title48-vol1/CFR-2011-title48-vol1-part4subpart4-4>

13. Federal Acquisition Regulations (FAR) section 52.204-2 - Security Requirements. <https://www.gpo.gov/fdsys/pkg/CFR-2002-title48-vol2/pdf/CFR-2002-title48-vol2-sec52204-1.pdf>
14. NIST FIPS 199: Standards for Security Categorization of Federal Information and Information Systems, dated February 2004.
<http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>
15. NIST SP 500-292: NIST Cloud Computing Reference Architecture, dated September 2011. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505
16. NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations, Revision 4, dated April 2013.
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
Note: <http://csrc.nist.gov/publications/PubsSPs.html> contains additional documents relating to SP 800-53.
17. NIST SP 800-59: Guideline for Identifying an Information System as a National Security System, dated August 2003.
<http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf>
18. NIST SP 800-66, Revision 1: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, dated October 2008. <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>
19. NIST SP 800-88, Revision 1: Guidelines for Media Sanitization, dated September 2012.
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>
20. NIST SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), dated April 2010.
<http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>
21. NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing, dated December 2011.
<http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>
22. NIST SP 800-145: The NIST Definition of Cloud Computing, dated September 2011. <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
23. NIST SP 800-37, Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems, dated February 2010.
<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>

24. NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, dated June 2015.
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf>
25. CNSS Instruction 4009: National Information Assurance (IA) Glossary, dated 30 April 2010. <https://www.cnss.gov> or www.cnss.gov/cnss/issuances/Instructions.cfm
26. CNSS Instruction 1253: Security Categorization and Control Selection for National Security Systems, dated 27 March 2014. <https://www.cnss.gov> or www.cnss.gov/cnss/issuances/Instructions.cfm
27. CNSS Instruction No.1253F, Attachment 5: Classified Information Overlay dated 09 May 2014. <https://www.cnss.gov> or www.cnss.gov/cnss/issuances/Instructions.cfm
28. CNSS Instruction No.1253F, Attachment 6: Privacy Overlay dated 20 April 2015. <https://www.cnss.gov> or www.cnss.gov/cnss/issuances/Instructions.cfm
29. DoD Chief Information Officer, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, 15 December 2014.
http://iase.disa.mil/Documents/commercial_cloud_computing_services.pdf
30. DoD Instruction 8500.01: Cybersecurity, dated 14 March 2014.
http://dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
31. DoD Instruction 8510.01: Risk Management Framework (RMF) For DoD Information Technology (IT), dated 12 March 2014.
http://dtic.mil/whs/directives/corres/pdf/851001_2014.pdf
32. DoD Instruction 8520.03: Identity Authentication for Information Systems, dated 13 May, 2011. <http://dtic.mil/whs/directives/corres/pdf/852003p.pdf>
33. DoD Instruction 8550.01: DoD Internet Services and Internet-Based Capabilities, September 11, 2012.
<http://www.dtic.mil/whs/directives/corres/pdf/855001p.pdf>
34. DoD Instruction 8551.01: Ports, Protocols, and Services Management (PPSM), May 28, 2014. <http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf>
35. DoD Instruction 8410.01, Internet Domain Name Use and Approval, dated April 14, 2008. <http://www.dtic.mil/whs/directives/corres/pdf/841001p.pdf>
36. DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations"
<http://www.dtic.mil/whs/directives/corres/pdf/853001p.pdf>
37. DoD Joint Publication 3-12 (R), "Cyberspace Operations"
http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

38. DoD Instruction 8582.01, Security of Unclassified DoD Information on Non-DoD Information Systems, June 6, 2012.
<http://www.dtic.mil/whs/directives/corres/pdf/858201p.pdf>
39. DoD Instruction 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense
<http://www.dtic.mil/whs/directives/corres/pdf/832007p.pdf>
40. DoD 5220.22-R: Industrial Security Regulation (ISR), dated December 1985.
<http://www.dtic.mil/whs/directives/corres/pdf/522022r.pdf>
41. DoD Instruction 5220.22: National Industrial Security Program, dated March 2011. <http://www.dtic.mil/whs/directives/corres/pdf/522022p.pdf>
42. DoD Manual 5220.22 Manual: National Industrial Security Program: Operating Manual (NISPOM), dated march 2013.
<http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf>
43. DoD Instruction 5200.01: DoD Information Security Program and Protection of SCI, dated June 2011.
<http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf>
44. DoD Manual 5200.01 Vol 1: DoD Information Security Program: Overview, Classification and Declassification, dated February 2012.
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf
45. DoD Manual 5200.01 Vol 2: DoD Information Security Program: Marking of Classified Information, dated March 2013.
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf
46. DoD Manual 5200.01 Vol 3: DoD Information Security Program: Protection of Classified Information, dated March 2013.
http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf
47. DoD Instruction 5200.02: DoD Personnel Security Program (PSP), Change 1 dated September 2014.
http://www.dtic.mil/whs/directives/corres/pdf/520002_2014.pdf
48. DoD Manual 5200.2-R: Personnel Security Program, dated February 1996.
<http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf>
49. CJCSM 6510.01B: Chairman of the Joint Chiefs of Staff Manual: Cyber Incident Handling Program, dated 10 July 2012. (Current as of 18 December 2014). http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf
50. DSS Facility Clearance Branch.
http://www.dss.mil/isp/fac_clear/fac_clear.html
51. DoD ECA PKI Certificate. <http://iase.disa.mil/pki/eca/Pages/index.aspx>

52. OPM Position Designation System 2010.
<http://www.opm.gov/investigations/background-investigations/position-designationtool/oct2010.pdf>
53. Federal Risk and Authorization Management Program (FedRAMP) Home Page.
<https://www.fedramp.gov/>
54. FedRAMP Control Specific Contract Clauses v2, June 6, 2014.
<http://www.fedramp.gov/resources/documents>
55. Defense Information Systems Agency, the Security Technical Implementation Guide (STIG) Home Page. <http://iase.disa.mil/stigs/Pages/index.aspx>
56. Defense Information Systems Agency, DoD Cloud Services Support website.
<http://disa.mil/Services/DoD-Cloud-Broker>
57. Guide to Understanding FedRAMP.
<https://www.fedramp.gov/resources/documents/>
58. FedRAMP Continuous Monitoring Strategy Guide.
<https://www.fedramp.gov/resources/documents/>
59. FedRAMP Control Specific Contract Clauses v2, June 6, 2014.
<https://www.fedramp.gov/resources/documents/>
60. OPM Position Designation System document, Oct 2010.
<http://www.opm.gov/investigations/background-investigations/position-designationtool/oct2010.pdf>
61. OPM Position Designation Tool.
<http://www.opm.gov/investigations/background-investigations/position-designation-tool/>
62. DoD DMZ STIG.
https://powhatan.iiee.disa.mil/stigs/downloads/zip/fouo_dod_internetnprnet_dmz_technology_v3r3_stig.zip (CAC/PKI required)

付録 B 用語集

B.1 クラウドの用語

このセクションはトピック別にまとめられている。

クラウドサービスプロバイダ (CSP) : クラウドサービスを提供する、商用またはプライベートな組織。特に記載がない場合には、クラウドサービスプロバイダ、DoD または Non-DoD のいずれかまたはすべてを示す。

商用 CSP : Non-DoD、Non 連邦政府組織が、ビジネスベンチャーの一環として、一般的には利益を得るための料金を徴収して、一般・政府の顧客にクラウドサービスを提供することを示す。

DoD CSP : DoD が所有し運用しているかまたはある部門 (例えば milCloud) の便益のために DoD の契約業者によるクラウドサービスの提供を示す。そのようなサービスは通常、コスト回収モデルのもとで提供される。DoD CSP は、Non-DoD ミッションパートナーを対象にクラウドサービスを提供することもある。

Non-DoD CSP : 商用または連邦政府が所有・運営する CSP を示す。

クラウドサービスの提供 (CSO) : CSP の製品またはサービスの提供を示す。言い換えれば、CSO は、CSP によって提供される実際のサービスとしてのインフラストラクチャ (IaaS)、サービスとしてのプラットフォーム (PaaS)、またはサービスとしてのソフトウェア (SaaS) ソリューションである。CSP は複数の CSO (たとえば、Microsoft 0-365 (SaaS) および Azure (I/PaaS)) を提供することができる。CSO はまた、任意のサービスタイプ (例えば、PaaS の下で顧客の使用のために任意に利用可能な 1 つまたは複数の特定のデータベースアプリケーション) 内で利用可能なオプションのサービスまたはソフトウェアの粒度を指す。

- ・ **サービスとしてのインフラストラクチャ (IaaS) :** NIST SP 800-145 で定義されているように、提供される機能は、利用者が任意のソフトウェアを展開して実行できる処理、ストレージ、ネットワーク、その他の基本的なコンピューティングリソースであり、これにはオペレーティングシステムとアプリケーションを含む。利用者は、基盤となるクラウドインフラストラクチャを管理または制御するのではなく、オペレーティングシステム、ストレージ、および展開されたアプリケーションを制御し、限定的に選択されたネットワークのコンポーネント (例えば、ホストファイ

アウオール) の制御が可能である。

- ・ **サービスとしてのプラットフォーム (PaaS)** : NIST SP 800-145 で定義されているように、提供される機能は、プロバイダから配布されたプログラミング言語、ライブラリ、サービス、ツールを使用し、利用者が作成または取得したアプリケーションをクラウドインフラストラクチャへ実装する形態である。利用者は、ネットワーク、サーバー、オペレーティングシステム、ストレージなどの基盤となるクラウドインフラストラクチャを管理または制御することはないが、導入されたアプリケーションやアプリケーションホスティング環境の構成や設定を制御できる。
- ・ **サービスとしてのソフトウェア (SaaS)** : NIST SP 800-145 で定義されているように、提供される機能は、クラウドインフラストラクチャ上で実行されているプロバイダのアプリケーションの利用である。アプリケーションは、ウェブブラウザ (例えば、ウェブベースの電子メール) のようなシンククライアントインタフェースまたはプログラムインタフェースを介して、様々なクライアント・デバイスからアクセス可能である。利用者は、ネットワーク、サーバー、オペレーティングシステム、ストレージ、さらには個々のアプリケーション機能を含む基盤となるクラウドインフラストラクチャを管理したり制御したりすることはできない。

コミュニティクラウド : 特定のグループまたは独立した顧客組織による排他的利用のためにサービスが提供されるマルチテナントクラウド。

連邦政府コミュニティクラウド : 複数の連邦政府機関 (DoD を含む) が利用できるコミュニティクラウド。クラウドサービスを提供するリソースは、連邦政府の使用に専念し、連邦以外の顧客からの物理的分離が必要である。

プライベートクラウド : 特定の顧客組織の排他的使用のためにサービスが提供される単一または複数のテナントクラウド。

DoD プライベートクラウド/CS0 : DoD コミュニティクラウドや CS0 で、1 または複数の DoD 顧客組織の占有的使用のためにサービスが提供されている。複数の DoD テナントや DoD がスポンサーであるテナントを同じクラウドでサポートしている。DoD は、クラウドサービスの使用に対する最終的な権限を保持し、Non-DoD がサービスを利用するには、DoD が後ろだてとなって承認されなければならない。クラウドサービスを提供するリソースは、DoD 専用の利用であり、DoD 専用ではないリソースから物理的に分離されている必要がある。

DoD クラウドサービスカタログ¹¹² : DoD コンポーネントが利用できる、セキュリティ・パッケージを有し、DoD の PA を取得したすべての CSO のリポジトリ。

DoD コンポーネント : DoD のサービスまたは機関（サブ機関/コマンド/組織を含む）。

DoD オフプレミス : オフプレミスとは施設（建物/コンテナ）や IT インフラストラクチャが、物理的にまたは仮想的に DoD の所有や管理する資産（すなわち、物理的や仮想的なオンプレミス）でない場合である。詳細については、セクション 5.2.1.1 「DoD オフプレミス対オンプレミス対仮想オンプレミス」を参照

DoD オンプレミス : オンプレミスとは施設（建物/コンテナ）や IT インフラストラクチャが、物理的に DoD の所有または管理された所有地にある場合である。つまり、DoD の要員と DoD セキュリティポリシーの直接コントロール下にあり、保護された周辺部（壁または「フェンス網」）内の DoD の施設（ベース、キャンプ、ポスト、基地（B/C/P/S）または借用の商用スペース）である。詳細については、セクション 5.2.1.1 の「DoD オフプレミス対オンプレミス対仮想オンプレミス」を参照。

DoD 仮想オンプレミス : 連邦政府や商用データセンターなどの物理的にオフプレミスな IT インフラストラクチャ（例えば、Non-DoD のセキュリティポリシーを使用して Non-DoD の人員が直接管理する施設）は、事実上特定の条件下で仮想オンプレミスとみなされる。これらの条件では、特定の物理的セキュリティ管理策が適用され、DISN 認定の境界が拡張される。本質的に、この構成は、インフラの周りに DoD で保護された境界線または「フェンスライン」の事実上の拡張である。詳細および要件については、セクション 5.2.1.1 「DoD オフプレミス、オンプレミス、仮想オンプレミス」を参照。

ミッションオーナー (MO) : ミッションオーナーは、DoD コンポーネント/機関の中の IT システム/アプリケーションの所有者/オペレーターまたはプログラマネージャーなどであり、1 つ以上の情報システムとアプリケーションをインスタンス化して運用し、IT ミッション達成のために CSP の CSO を活用することもある。ミッションオーナーは、コンポーネント/機関レベルの方針や取得の管理を監督していることがあるが、この文脈ではミッションオーナーは DoD エンタープライズや DoD コンポーネント/機関エンタープライズではな

¹¹² DoD Cloud Service Catalog:

<https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Approved-Commercial.aspx> (DoD CAC/PKI required)
<http://www.disa.mil/~media/Files/DISA/Services/Cloud-Broker/AuthorizedCloudServicesCatalog.pdf> (Public)

い。ミッションオーナーはまた、情報の所有者および情報システムの A0 に対しても責任がある。情報所有者は、情報および関連するすべての派生物を所有することに加えて、クラウドに移行されるデータが、リスク管理エグゼクティブ/A0 の承認を得た適切なセキュリティレベルであることを保証する責任がある。

B2 一般的な用語

真正性：CNSSI-4009 で定義されているように、「本物であり、検証され、信頼できるメッセージ、またはメッセージ発信者の妥当性に対する信頼」

可用性：CNSSI-4009 で定義されているように、「許可されたエンティティの要求に応じて、アクセス可能で利用できるという性質」

格付け情報：CNSSI-4009 で定められるように、「文書の状態であるとき、無許可の開示からの保護を必要とする大統領令 13526 や、これに先行した命令に従って決定され、格付けされた状態を示すためにマークされた情報」

C/CE (Control/Control Enhancement)：さまざまなベースラインとオーバーレイで選択され組み立てられた、国立標準技術研究所 (NIST) の Special Publication (SP) 800-53 セキュリティとプライバシーコントロールとその拡張機能。

CSM：クラウドセキュリティモデル。CSM は、CC SRG に先行した文書であるが、その後廃止された。

CSSP：サイバーセキュリティサービスプロバイダ。DoDI 8530.01 で定義された DoD の情報ネットワーク運用をサポートするサイバーセキュリティ活動。

専用インフラストラクチャ：単一の顧客組織または特定の顧客グループ（特定のコミュニティなど）にサービスを提供することに専念するクラウドサービスインフラストラクチャを示す。

機密性：CNSSI-4009 で定義されているように、「情報にアクセスする権限がない限り、情報がシステムエンティティ（ユーザ、プロセス、デバイス）に開示されないという性質」

サイバーインシデント：情報システム内の情報へ、実際または潜在的に悪影響をもたらすコンピュータネットワークの使用によって行われるアクション。インシデントを参照。

インシデント：情報システムの機密性、完全性、可用性；またはシステムのプロセス、保存、送信する情報；またはセキュリティポリシー、セキュリティ手順、許容される使用ポリシーに対する違反による差し迫った脅威で、実際または潜在的に危険にさらすと評価された事案

完全性：CNSSI-4009 で定義されているように「エンティティが許可されていない方法で変更されていないという性質」

JAB(Joint Authorization Board)：共同認証委員会。FedRAMP プログラムの主要なガバナンスと意思決定の機関

ミッションオーナー：DoD クラウドの利用者。NIST SP 500-292 で定義されているように、「クラウド利用者は、クラウドプロバイダとビジネス関係を維持し、クラウドプロバイダから提供されるサービスを利用する個人または組織を示す。」

否認拒否：CNSSI-4009 で定義されているように、「情報の送信者に配信証明が提供され、受信者に送信者の身元証明が提供されて、両者とも後で情報を処理したことを否定できない保証」

暫定認可 (PA : Provisional Authorization)：連邦政府や DoD の情報および情報システムをホストする民間 CSO を事前に認定するために、DoD および FedRAMP が使用する事前取得型のリスク管理フレームワーク情報システム認可。PA は、RMF のもとでの請負業者の選定とそれに続くシステム認証の際に、連邦および DoD クラウドミッションオーナーによって利用される。2.6 節の DoD 暫定認可を参照

RMF：リスク管理フレームワーク。NIST SP 800-37 に記載されているように、RMF は、情報システムセキュリティに対する 6 段階のリスクベースのアプローチであり、その目的は FISMA を含む様々な公法の遵守である。RMF は、伝統的な C&A(certification and accreditation)プロセスを置き換える。

修復：元の、正常な、または障害のない状態への復帰

SCA(Security Control Assessor)：セキュリティ管理策査定者。NIST SP 800-37 で定義されているように、「セキュリティ管理策の査定を担当する個人、グループ、または組織」

流出またはデータ流出:格付けされた情報やCUI(Controlled Unclassified Information)の情報が、当該データに適用可能なセキュリティレベルで認定されていない情報システムへ不正に転送されること。

付録C 役割と責任

表7はCC SRGにおける主要な役割と責任の割り付けを示すものである。

表7 役割と責任

役割	責任
DISA	<ul style="list-style-type: none">• DoD クラウドコンピューティングのセキュリティ要件ガイドライン (SRG) とセキュリティ技術実装ガイダンス (STIG) の提供• 国防総省の暫定的認可を受ける上で考慮すべき CSP のサービス提供と 3PAO の結果の評価• DoD 暫定認可の発行• DoD 境界クラウドアクセスポイント (BCAP) の開発と維持• 境界サイバースペース防衛 (BCP) の提供• DoD CIO の FedRAMP Joint Authorization Board に対する技術的サポートの提供• DoD クラウドサービスカタログの提供• 商用クラウドサービスを使用した DoD コンポーネントのレジストリの維持• DoDIN 免除プロセスのサポート• CSP の継続的な監視結果の受領と DoD 内の関連エンティティへの引き渡し• DoD CSSP 認証者としての役割
クラウドサービスプロバイダ (CSP)	<ul style="list-style-type: none">• クラウドサービスを提供する商用ベンダーまたは連邦機関 (DoD CSP を含む)• ミッションで利用するためのクラウドサービスの提供• インフラやサービスの提供に対するサイバーセキュリティサービスの提供
クラウドアクセスポイント (CAP)	<ul style="list-style-type: none">• DISA または他の DoD コンポーネントによって提供される。• CSP 環境での運用に影響を与える脆弱性やリスクからの DoD ミッションの保護• 商用クラウドサービスでホストされているアプリケーションの境界防御とセンシングの提供
DoD 最高情報責任者	<ul style="list-style-type: none">• すべての CAP に対する承認権者

(DoD CIO)	
FedRAMP 統合認証委員会 (JAB)	<ul style="list-style-type: none"> • FedRAMP プログラムに基づく CSP セキュリティ評価パッケージのレビュー • FedRAMP 暫定認可の付与 • FedRAMP 暫定認可の定期的な見直と更新の保証 • 第三者評価機関 (3PAO) の認定基準の承認
第三者評価機関 (3PAO)	<ul style="list-style-type: none"> • アメリカン・アソシエーション・ラボラトリーによる認定 • 認定 (A2LA) と FedRAMP PMO による最終承認 • CSP からの契約 • CSP クラウドオフリングのセキュリティアセスメントを独立して実行し、FedRAMP 要件に従ったセキュリティアセスメントパッケージ成果物の作成 • CSP システムの継続的な監視の実行 • DoD FedRAMP +のセキュリティマネジメントやその他の要件に対する CSP の遵守状況の独立した評価
DISA クラウド SCA	<ul style="list-style-type: none"> • 3PAO によって実施されない場合、DoD FedRAMP +セキュリティマネジメントとその他の要件に対する CSP の遵守状況の独立した評価 • DoD CSA の FedRAMP セキュリティマネジメントに対する CSP の遵守状況の評価 (他の DoD SCA による評価が行われていない場合) • FedRAMP 以外の DoD の評価を受けている商用 CSP の FedRAMP セキュリティマネジメントに対する CSP の遵守状況の評価 (他の DoD SCA によって行われていない場合) • CSA SAR の評価と認証勧告の策定を通じ、PA の取得に関する DISA A0 への助言 • DoD CIO の FedRAMP テクニカルアドバイザーとして、JAB トライチェアとしての役割
DISA クラウド SCA (DSIA 以外)	<ul style="list-style-type: none"> • DoD PA やコンポーネント機関 ATO に付与するために FedRAMP 以外の DoD の評価を受けている DoD または Non-DoD CSP の FedRAMP および FedRAMP +セキュリティ管理策に対する CSP の遵守を評価することができる。(DISA が実施していない場合)
DISA 認可当局 (A0)	<ul style="list-style-type: none"> • DoD が使用する CSP のサービス提供に対する PA の公式な承認
DoD コンポーネント認可当局 (A0)	<ul style="list-style-type: none"> • ミッションオーナーのシステム/アプリケーションのための ATO の承認者 • 残存リスクを理解するための PA 文書のレビュー

<p>ミッションオーナー</p> <p>(CSP の DoD クラウド顧客 DoD のクラウド顧客)</p>	<ul style="list-style-type: none"> ・ ミッションをサポートするためのクラウドサービスを取得する DoD エンティティ ・ 残存リスクを理解するための DoD PA 文書のレビュー ・ ミッションシステム/アプリケーションへ ATO を発行するためのアセスメントの実施 ・ ミッションサイバースペースディフェンス (MCD) サービスプロバイダが特定され、予算が用意されていることの確認 ・ ミッションシステム/アプリケーションのエンドポイントサイバースペースディフェンスの実行 ・ サイバースペースの CSP 要件を確実にする DoD やその他の SRG 要件がクラウド契約に含まれていることの確認 ・ ポートとプロトコルの PPSM オフィスへの登録
<p>国土安全保障省 (DHS) 米国コンピュータ緊急準備チーム (US-CERT)</p>	<ul style="list-style-type: none"> ・ FedRAMP が義務づけている CSP からのインシデント報告の受領 ・ Non-DoD 機関間の調整 <p>(US-CERT:US-Computer Emergency Readiness Team)</p>
<p>コンピュータネットワーク防衛サービスプロバイダ (CDSP)</p>	<ul style="list-style-type: none"> ・ ネットワークの保護、脅威の検出、インシデントへの対応に対処するサイバー防衛サービスと指揮統制 (C2) の提供
<p>サイバーセキュリティサービスプロバイダ (CSSP)</p>	<ul style="list-style-type: none"> ・ ネットワークの保護、脅威の検出、およびインシデントへの対応について、サイバーセキュリティサービスの提供
<p>境界サイバースペースディフェンス (BCD) アクションを実行する組織</p> <ul style="list-style-type: none"> ・ DoD CSSPs 	<ul style="list-style-type: none"> ・ 境界クラウド・アクセス・ポイント (BCAP) で、オフプレミス CSP との接続の監視と防御 ・ SP 横断の分析機能またはエンティティの提供 ・ DCD、BCD、および MCD アクションを実行する組織とのコミュニケーション ・ BCD で収集した MCD に関連した兆候や警告を、タイムリーに MCD へ提供
<p>ミッションサイバースペースディフェンス (MCD) アクションを実行する組織</p> <ul style="list-style-type: none"> ・ DoD CSSP 	<ul style="list-style-type: none"> ・ 特定のミッションオーナーのシステム/アプリケーションや仮想ネットワークに対するサイバースペース防衛サービスの提供 ・ ミッションオーナーの DoD サイバースペース防衛の窓口としての役割 ・ DCD、BCD、MCD アクション、ミッションオーナーを務めている組織とのコミュニケーション

付録D PA の CSP 評価パラメータ値

表 8 は、FedRAMP および FedRAMP+ C/CE の中でパラメータ値を必要とする項目だけの一覧を示している。これらの C/CE と関連するパラメータ値は、ここでは CSP のベンチマークとして公開され、PA の受領に向けた CSP 評価に使用される。CSP が満たさなければならないすべての FedRAMP 中 (moderate) と FedRAMP+ C/CE の完全なリストではない。完全な C/CE テキストは、対象としている選択または値の文脈を提供するために含まれている。

多くのパラメータ値は、DoD または FedRAMP で定義されていないため、CSP 組織や CSO によって変更される可能性がある。このため、この SRG では、すべてのケースで全部のパラメータ値を定義することは不可能である。表 8 において、左側の列のパラメータに対する右側の列の参照がない項目が定義されていないパラメータ値であり、これらに関しては CSP がセキュリティ計画の中で、C/CE が DoD のアセスメントと DoD PA のために、DISA AO の認定／承認にどのように適合させるか詳細化し、パラメータ値を定義しなければならない。

注：一部の C/CE については、必要なパラメータの選択/値は DoD または FedRAMP によって定義されていなかった。そのような項目については、表の右の列セルは空白である。関連付けられたパラメータ値は、上記に示したように、アセスメントのために CSP が値を定義するものとして扱われる。

多くの場合、DoD と FedRAMP はコントロールパラメータに異なる値を定義している。そのような場合、表示されているように、影響レベル 4-6 の DoD PA に対してより厳しいパラメータ値が必要となる。影響レベル 2 の CSO については、FedRAMP の値を用いて評価される。影響レベル 4-6 とレベル 2 を比較して値が異なるパラメータのコントロールは、表に注記されている。CSP は、検討の結果としてコントロールを満たす別の値や方法を提供可能である。

注：レベル 6 の場合、CNSSI 1253 格付け情報オーバーレイのアプリケーションは、次の表に示されている値のいくつかを変更する。オーバーレイ値が優先である。

ミッションオーナーは、DoD RMF TAG (Technical Advisory Group) で定義された値に従い IaaS/PaaS クラウドサービスでインスタンス化するアプリケーションのパラメータ値を使用、定義、調整する必要がある。DoD PA の取得で評価された DoD/FedRAMP の定義済みと CS が定義したパラメータ値は、ミッションオーナーのシステム/アプリケーションで継承される。ミッションオーナーがこれらの継承された値の変更を必要とする場合は、CSP と交渉し、SLA/契約へ変更を反映する必要がある。

注：DoD コンポーネント/ミッションオーナーは、RFP を発して契約を実行する際に、既定の値の変更や、追加の選択/値を定義してこの値のセットを調整できる。ミッションオーナーは、CSP のセキュリティプランに記載されている値を受け入れて PA に反映されている DISA AO を受け入れるか、または交渉によって決めた別の値を契約/SLA に含める必要がある。

表 8 PA アセスメントのための FedRMP M/FedRMP+コントロール/強化：パラメータ値

コントロール/強化：テキスト	値
<p>AC-1; アクセス制御; アクセス制御ポリシーと手順:</p> <p>組織:</p> <p>a. 開発、文書化、配布</p> <p>[設定: 組織が定めた要員または役割]:</p> <p>1. アクセス制御ポリシーは、目的、範囲、役割、責任、管理コミットメント、組織エンティティ間の調整、コンプライアンスに言及。</p> <p>2. アクセス制御ポリシーおよび関連するアクセス制御の実施を促進する手順。そして</p> <p>b. 次の現状のレビューと更新:</p> <p>1. アクセス制御ポリシー</p> <p>[設定: 組織が定めた頻度];</p> <p>2. アクセス制御手順</p> <p>[設定: 組織が定めた頻度].</p> <p>参照: NIST Special Publications 800-12、800-100.</p>	<p>AC-1</p> <p>影響レベル 4-6:</p> <p>a. すべての人員</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2:</p> <p>b. 1 少なくとも 3 年ごと</p> <p>すべての影響レベル:</p> <p>b. 2 少なくとも年に 2 回</p> <p>根拠: FedRAMP v2</p> <p>-----</p>
<p>AC-2; アクセス制御; アカウント管理:</p> <p>組織:</p>	<p>AC-2</p>

<p>a. 組織のミッション/ビジネス機能をサポートするため、以下のタイプの情報システムアカウントを識別して選択</p> <p>[設定：組織が定めた情報システムアカウントタイプ];</p> <p>b. 情報システムアカウントのアカウントマネージャーの割り当て</p> <p>c. グループメンバーとロールメンバーシップの条件の設定</p> <p>d. 各アカウントの情報システム、グループおよびロールのメンバーシップ、アクセス権限（特権）とその他の属性（必要に応じて）の許可ユーザを指定</p> <p>e. 承認が必要</p> <p>[設定：組織が定めた要員または役割]</p> <p>情報システムアカウントを作成する要求の場合</p> <p>f. 情報システムアカウントを作成、有効化、変更、無効化、削除</p> <p>[設定：組織が定める手順または条件]</p> <p>g. 情報システムアカウントの使用を監視</p> <p>h. アカウントマネージャーへ通知：</p> <ol style="list-style-type: none">1. アカウントが不要になった場合2. ユーザの解除または転勤 そして3. 個々の情報システムの仕様や need-to-know の変更； <p>i. 以下に基づいた情報システムのアクセス許可</p> <ol style="list-style-type: none">1. 正規のアクセス許可；2. 意図したシステムの使用；そして3. 組織または関連するミッション/ビジネス機能に必要とされるその他の属性； <p>j. アカウント管理要件に準拠したレビュー</p> <p>[設定：組織が定めた頻度]；そして</p>	<p>影響レベル 4-6：</p> <p>e. ISSM または ISSO</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル：</p> <p>j. 少なくとも年に 1 回</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
--	--

<p>k. 要員がグループから削除されたときに、共有/グループアカウントの資格情報を再発行するプロセス（発行されている場合）の確立。</p> <p>参照：なし</p>	
<p>AC-2 (2) ; アクセス制御; アカウント管理 - 強化 :</p> <p>一時的な緊急アカウントの解除</p> <p>情報システムは自動的に</p> <p>[選択 :</p> <ul style="list-style-type: none">- 削除;- 無効化 <p>]</p> <p>一時的および緊急アカウント</p> <p>[設定：各タイプのアカウントに対する組織が定めた期間]</p> <p>参照：なし</p>	<p>AC-2 (2)</p> <p>影響レベル 4-6 :</p> <p>一時的なユーザアカウント : 72 時間</p> <p>緊急管理者アカウント : never (補足勧告を参照)</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2 :</p> <p>[一時的や緊急アカウントでは 30 日以内]</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>
<p>AC-2 (3) ; アクセス制御; アカウント管理 - 強化 :</p> <p>非アクティブなアカウントの無効化</p> <p>情報システムによる非アクティブなアカウントの自動的な無効化</p> <p>[設定：組織が定めた期間].</p> <p>参照：なし</p>	<p>AC-2 (3)</p> <p>影響レベル 4-6 :</p> <p>35 日間</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2 :</p> <p>ユーザアカウントで 90 日間</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>

	<p>FedRAMP 追加要件とガイダンス：</p> <p>要件：サービスプロバイダは、非ユーザアカウント（たとえば、デバイスに関連付けられたアカウント）の期間を設定する。期間は認定当局に承認される。</p>
<p>AC-2（4）；アクセス制御；アカウント管理－強化：</p> <p>自動化された監査アクション</p> <p>情報システムは、アカウントの作成、変更、有効化、無効化、および削除操作を自動的に監査し、通知</p> <p>[設定：組織が定めた要員または役割].</p> <p>参照：なし</p>	<p>AC-2（4）</p> <p>影響レベル 4-6：</p> <p>システム管理者と ISSO</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>
<p>AC-2（5）；アクセス制御；アカウント管理－強化：</p> <p>非アクティブなログアウト</p> <p>組織は、ユーザが次の状態でログアウトを要求</p> <p>[設定：組織が定めた非アクティブな期間またはログアウトすべき時間の説明].</p> <p>参照：なし</p>	<p>AC-2（5）</p> <p>影響レベル 4-6：</p> <p>正式な組織ポリシーで別段の定めがない限り、ユーザの標準就業時間の終わりに</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>
<p>AC-2（7）；アクセス制御；アカウント管理－強化：</p> <p>役割に基づくスキーム</p> <p>組織は：</p> <p>a．許可された情報システムへのアクセスおよび権限を役割ベースとしたアクセス方式に従った、特権ユーザアカウントの確立と管理</p> <p>b．特権役割の割り当ての監視；そして</p>	<p>AC-2（7）</p>

<p>c. 次を実行</p> <p>[設定：組織が定めたアクション]</p> <p>特権ロールの割り当てが適切でなくなった場合</p> <p>参照：なし</p>	<p>影響レベル 4-6：</p> <p>c. 特権ユーザアカウントの無効化（または取り消し）</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>
<p>AC-2 (9)；アクセス制御；アカウント管理－強化：</p> <p>共有グループ/アカウントの使用に関する制限</p> <p>組織は、次に合致する場合のみに、共有/グループアカウントの使用を許可</p> <p>[設定：共有/グループアカウントの設定について組織が定めた条件].</p> <p>参照：なし</p>	<p>AC-2 (9)</p> <p>すべての影響レベル：</p> <p>監査とアカウントビリティをサポートするために、ユーザの利用状況をアカウントに一意的に帰属させる要件が実装されていない限り、共有/グループアカウントは許可されない。例外はケースバイケースで承認される場合がある。個人アカウントは共有されない。</p> <p>根拠：DoD ベストプラクティス、SRG と STIG、CNSSI 1253 プライバシー・オーバーレイ</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>共有/グループアカウントを展開する場合に必要</p>
<p>AC-2 (12)；アクセス制御；アカウント管理－強化：</p> <p>アカウントの監視/異常な使用</p> <p>組織：</p> <p>a. 次について、情報システムのアカウントを監視</p> <p>[設定：組織が定めた非典型的な使用]；</p>	<p>AC-2 (12)</p>

<p>b. 情報システムアカウントの異常な使用の報告</p> <p>[設定：組織が定めた要員または役割].</p> <p>参照：なし</p>	<p>影響レベル 4-6：</p> <p>b. 少なくとも、ISSO</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル：</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>AC-2 (12) (a) および AC-2 (12) (b) 追加の FedRAMP 要件およびガイダンス：特権アカウントに必要とされる。</p>
<p>AC-4；アクセス制御；情報フローの強制：</p> <p>情報システムによる、システム内および相互接続されたシステム間の情報の流れを制御するために承認された権限の強制</p> <p>[設定：組織が定めた情報フロー制御ポリシー].</p> <p>参照：Web：ucdmo.gov</p>	<p>AC-4</p> <p>[値は未設定。 CSP により設定される]</p>
<p>AC-4 (21) ； アクセス制御；情報フローの強制 - 強化：</p> <p>情報フローの物理的/論理的分離</p> <p>情報システムは、次により情報フローを論理的または物理的に分離</p> <p>[設定：組織が定めたメカニズムおよび/または技術]</p> <p>次を達成するために</p> <p>[設定：組織が定めた情報の種類に応じた分離].</p> <p>参照：なし</p>	<p>AC-4 (21)</p> <p>[値は未設定。 CSP により設定される]</p>

<p>AC-5; アクセス制御; 職務の分離:</p> <p>組織:</p> <p>a. 次を分離</p> <p> [設定: 組織の定めた要員の職務];</p> <p>b. 要員の職務の分離を文書化する。そして</p> <p>c. 職務の分掌を補助するような情報システム</p> <p>アクセス権限の定義</p> <p>参照: なし</p>	<p>AC-5</p> <p>[値は未設定。 CSP により設定される]</p>
<p>AC-6 (1) ; アクセス制御; 最小特権 - 強化:</p> <p>セキュリティ機能へのアクセス許可</p> <p>組織は、次のアクセスを明示的に許可</p> <p> [設定: 組織が定めたセキュリティ機能 (ハードウェア、ソフトウェア、およびファームウェアに実装された) やセキュリティ関連情報].</p> <p>参照: なし</p>	<p>AC-6 (1)</p> <p>影響レベル 4-6 :</p> <p>すべての機能は一般にアクセス不可であり、セキュリティ関連の情報はすべて非公開</p> <p>根拠: DoD RMF TAG</p> <p>-----</p>
<p>AC-6 (2) ; アクセス制御; 最小特権 - 強化:</p> <p>非セキュリティ機能に対する非特権アクセス</p> <p>組織では、次をアクセスする情報システムアカウントまたはロールのユーザが</p> <p> [設定: 組織が定めたセキュリティ機能またはセキュリティ関連情報]</p> <p>セキュリティ以外の機能にアクセスするときは、特権のないアカウントまたはロールを使用</p>	<p>AC-6 (2)</p> <p>すべての影響レベル:</p> <p>すべてのセキュリティ機能</p> <p>根拠: FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス:</p> <p>AC-6 (2) ガイダンス: セキュリティ機能の例; システムアカウントの確立、アクセス許可 (例えばアクセス権、特権) の設定、監査対象イベントの設定、侵入検知パラメータの設定、システムプログラミング、システムとセキュリティ管理策、その他の特権機能</p>

<p>AC-6 (5) ; アクセス制御; 最小特権 - 強化:</p> <p>特権アカウント</p> <p>組織は、次に対し情報システムの特権アカウントを制限</p> <p>[設定: 組織が定めた要員または役割].</p> <p>参照: なし</p>	<p>AC-6 (5)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>AC-6 (7) ;アクセス制御; 最小特権 - 強化: ユーザ権限のレビュー</p> <p>組織:</p> <p>a. レビュー</p> <p>[設定: 組織が定めた頻度]</p> <p>割り当てられた特権</p> <p>[設定: 組織が定めた役割またはユーザのクラス]</p> <p>そのような特権の必要性を検証—そして</p> <p>b. 必要に応じ、組織のミッション/ビジネスニーズを正しく反映するための特権の再割り当てまたは削除</p> <p>参照: なし</p>	<p>AC-6 (7)</p> <p>影響レベル 4-6 :</p> <p>a. 毎年最低でも</p> <p>a. すべてのユーザ</p> <p>根拠: DoD RMF TAG</p> <p>-----</p>
<p>AC-6 (8) ;アクセス制御; 最小特権- 強化: コード実行のための権限レベル</p> <p>情報システムは、次を防止</p> <p>[設定: 組織が定めたソフトウェア]</p> <p>ソフトウェアを実行しているユーザよりも高い権限レベルで実行することを禁止</p> <p>参照: なし</p>	<p>AC-6 (8)</p> <p>影響レベル 4-6 :</p> <p>明示的に文書化されたソフトウェアを除くすべてのソフトウェア</p> <p>根拠:</p> <p>DoD の RMF TAG</p> <p>-----</p>

<p>AC-7;アクセス制御; 失敗したログイン試行 :</p> <p>情報システム :</p> <p>a. 次の上限を強制</p> <p>[設定 : 組織が定めた回数]</p> <p>ユーザが連続して無効なログイン試行を</p> <p>[設定 : 組織が定めた期間];</p> <p>b. 自動的に</p> <p>[選択 :</p> <p>-アカウント/ノードをロック</p> <p>[設定 : 組織が定めた期間];</p> <p>-管理者によって解放されるまで、アカウント/ノードをロックする。</p> <p>-次のログインプロンプトを遅らせる</p> <p>[設定 : 組織が定めた遅延アルゴリズム]</p> <p>]</p> <p>成功しなかった試行の最大回数を超えたとき</p> <p>参照 : なし</p>	<p>AC-7</p> <p>影響レベル 2 :</p> <p>AC-7a [3 回以下]</p> <p>[1 5 分]</p> <p>AC-7b [アカウント/ノードを 3 0 分間ロック]</p> <p>根拠 : FedRAMP v2</p> <p>-----</p> <p>影響レベル 4-6 :</p> <p>a1. 3</p> <p>a2. 1 5 分</p> <p>b1. アカウント/ノードをロックする</p> <p>b2. 管理者によってリリースされるまで</p> <p>b3. 最低 5 秒</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p>
<p>AC-8;アクセス制御;システム使用通知 :</p> <p>情報システムは :</p> <p>a. 次をユーザに表示</p> <p>[設定 : 組織が定めたシステム使用のメッセージまたはバナーによる通知]</p> <p>システムへアクセスを許可する前に、連邦法大統領令、指令、方針、規制、基準、ガイダンスに準拠した、プライバシーとセキュリティ通知の提供</p> <p>1. ユーザは米国政府の情報システムにアクセスしている。</p> <p>2. 情報システムの使用状況を監視し、記録し、監査の対象とすることができる。</p>	<p>AC-8</p> <p>影響レベル 4-6 :</p> <p>a. CS0 には、最低 1300 文字のログオンバナーをサポートするためのカスタムによる設定可能な機能が必要。これは、特権ユーザおよび非特権ユーザにログオンプロンプトが表示される前に表示され、確認されることが必要</p> <p>c. a を参照</p> <p>ミッションオーナーのガイダンス : ログオンする必要があるすべての特権ユーザおよび非特権ユーザに対し、CS0 は DoDI 8500.01 Encl. 3, para 9. a. (1) (d)に従って、ミッション・アプリケーション、仮想</p>

<p>3. 情報システムの無断使用は禁止されており、刑事罰および民事罰の対象となる。そして</p> <p>4. 情報システムの使用は、監視と記録に同意することを示す。</p> <p>b. ユーザが使用条件を確認し、情報システムへのログオンまたはそれ以上のアクセスを明示的に行うまで、通知メッセージまたはバナーを画面に保持。そして</p> <p>c. 一般にアクセス可能なシステムの場合：</p> <ol style="list-style-type: none"> 1. 次のシステム使用情報を表示する。 [設定：組織が定めた条件]. さらなるアクセス許可に先立って； 2. これらの活動を禁止するようなシステムのプライバシー保護と合致した監視、記録、または監査への参照を表示する。そして、 3. システムの許可された使用の説明を含む。 <p>参照：なし</p>	<p>マシン、データベースなどにログオンする際のログオンバナー機能を提供する。</p> <p>根拠：DoD RMF TAG をクラウド向けに修正 -----</p> <p>すべての影響レベル： 追加の要件とガイダンスを参照</p> <p>根拠：FedRAMP v2 -----</p> <p>FedRAMP 追加要件とガイダンス： 要件：サービスプロバイダは、システム使用通知制御を必要とするクラウド環境の要素を決定しなければならない。システム使用通知を必要とするクラウド環境の要素は、承認当局（A0）によって承認され、受理される。 要件：サービス提供者は、システム使用通知の検証方法と、チェックの適切な周期を決定しなければならない。システム使用の通知と周期は A0 によって承認され受理される。 ガイダンス：コンフィギュレーション・ベースラインチェックの一部として実行される場合、チェックが行われ、合格（または失敗）のチェック設定が必要な項目の%が提供される。 要件：コンフィギュレーション・ベースラインチェックの一部として実行されない場合、検証結果をどのように提供するか、およびサービスプロバイダによる検証周期について、文書化された合意が必要である。 結果の検証を提供する方法に関する文書化</p>
--	---

	された合意は、A0 によって承認され、受理される。
AC-10; アクセス制御; 同時セッション制御 : 情報システムは、次についてそれぞれの同時セッションの数を制限する。 [設定 : 組織が定めたアカウントとアカウントタイプ] 次について [設定 : 組織が定めた数]. 参照 : なし	AC-10 影響レベル 4-6 : すべてのアカウントタイプとアカウント 根拠 : DoD RMF TAG ----- 影響レベル 2 : 特権アクセスのセッション数は 3、および非特権アクセスでは 2 根拠 : FedRAMP v2 -----
AC-11; アクセス制御; セッションロック : 情報システム : a. 次の期間セッションロックを開始することにより、システムへのさらなるアクセスの防止 [割当 : 組織が定めた期間] 非アクティブやユーザからの要求を受信したとき、そして b. 確立された識別および認証手順を使用し、ユーザがアクセスを再確立するまでセッションロックを保持 参考資料 : OMB 覚書 06-16.	AC-11 すべての影響レベル : a. 15 分 根拠 : DoD RMF TAG と FedRAMP v2 -----

<p>AC-12; アクセス制御; セッション終了:</p> <p>情報システムは次の後、自動的にユーザセッションを終了</p> <p>[設定: 組織が定めた条件またはセッションの切断が必要なトリガーイベント]</p> <p>参照: なし</p>	<p>AC-12</p> <p>[値は未設定。 CSP により設定される]</p>
<p>AC-14; アクセス制御; 識別または認証なしの許可されたアクション:</p> <p>組織:</p> <p>a 識別する</p> <p>[設定: 組織が定めたユーザの処理]</p> <p>組織のミッション/ビジネス機能と整合した、情報システムの識別や認証なしの実行; および</p> <p>b. 情報システムのセキュリティ計画において、識別や認証を必要としないユーザアクションであることの文書化と裏付けの根拠</p> <p>参照: なし</p>	<p>AC-14</p> <p>[値は未設定。 CSP により設定される]</p>
<p>AC-17 (3) ; アクセス制御; リモートアクセス - 強化:</p> <p>マネージドアクセスコントロールポイント</p> <p>情報システムは、すべてのリモートアクセスをルーティング</p> <p>[設定: 組織が定めた数]</p> <p>マネージドネットワークアクセス制御ポイント</p> <p>参照: なし</p>	<p>AC-17 (3)</p> <p>影響レベル 4-6 :</p> <p>レベル 4/5 : オフプレミスの CSP インフラは、1 つ以上の外部 DoDIN クラウドアクセスポイント (CAP) を介して DoD 顧客に接続する必要がある。</p> <p>レベル 4/5 : オンプレミス商用 CSP インフラは、1 つまたは複数の内部 DoDIN クラウドアクセスポイント (CAP) を介して DoD 顧客に接続する必要がある。DoD がすべての CSP のインフラまたはサービスの提供について定義するのは適切ではない。CSP が</p>

	<p>値を定義し、DISA AO が承認して受理する。</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p>
<p>AC-17 (4) ; アクセス制御; リモートアクセス - 強化 :</p> <p>特権コマンド/アクセス</p> <p>組織 :</p> <p>a. 次に限り、特権コマンドの実行を許可し、リモートアクセスを介したセキュリティ関連情報へのアクセスを許可</p> <p>[設定 : 組織が定めたニーズ];</p> <p>そして</p> <p>b. そのようなアクセスには、情報システムのセキュリティ計画で理由を文書化</p> <p>参照 : なし</p>	<p>AC-17 (4)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>AC-17 (9) ; アクセス制御; リモートアクセス - 強化 :</p> <p>アクセスの切断/無効化</p> <p>組織は、次の期間内に情報システムへのリモートアクセスを迅速に切断または無効にする機能を提供</p> <p>[設定 : 組織が定めた期間].</p> <p>参照 : なし</p>	<p>AC-17 (9)</p> <p>影響レベル 4-6 :</p> <p>直ちに</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2 :</p> <p>15 分以下</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>

<p>AC-19 (5) ; アクセス制御; モバイルデバイスのアクセス制御 - 強化: フルデバイス/コンテナベースの暗号化</p> <p>組織は、</p> <p>[選択:</p> <ul style="list-style-type: none">-フルデバイス暗号化。-コンテナの暗号化 <p>]</p> <p>次の情報の機密性と完全性を保護する</p> <p>[設定: 組織が定めたモバイルデバイス]</p> <p>参照: なし</p>	<p>AC-19 (5)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>AC-21; アクセス制御; ユーザベースのコラボレーションと情報共有 RENAMED: 情報共有:</p> <p>組織:</p> <p>a. 許可されたユーザが、共有パートナーに割り当てられたアクセス許可が、次の情報のアクセス制限と一致するかどうかを判断できるようにすることで、情報の共有を促進</p> <p>[設定: ユーザの裁量が必要な状況における組織が定めた情報共有];</p> <p>そして</p> <p>b. 利用</p> <p>[設定: 組織が定めた自動化されたメカニズムまたは手動プロセス]</p> <p>ユーザが情報共有/コラボレーションの決定を行う際の支え</p> <p>参照: なし</p>	<p>AC-21</p> <p>[値は未設定。 CSP により設定される]</p>

<p>AC-22; アクセス制御; 一般公開されているコンテンツ :</p> <p>組織 :</p> <p>a. 公衆がアクセス可能な情報システムに情報を投稿する権限を与えられた個人を指定</p> <p>b. 公開された情報の中に非公開情報を含むことがないよう教育</p> <p>c. 非公開の情報が含まれていないことを確認するために、公衆がアクセス可能な情報システムへ投稿する前に当該情報の内容をレビュー そして</p> <p>d. 公衆がアクセス可能な情報システムのコンテンツの中に非公開の情報がないかレビュー</p> <p>[設定 : 組織が定めた頻度]</p> <p>そのような情報が発見された場合は削除</p> <p>参照 : なし</p>	<p>AC-22</p> <p>影響レベル 4-6 :</p> <p>d. 90 日ごとまたは新しい情報が投稿されるたびに</p> <p>根拠 :</p> <p>DoD の RMF TAG</p> <p>-----</p> <p>影響レベル 2 :</p> <p>d. 少なくとも四半期ごと</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>
<p>AC-23; アクセス制御; データマイニング保護 :</p> <p>組織は、</p> <p>[設定 : 組織が定めたデータマイニング防止と検知技術]</p> <p>次を対象に</p> <p>[設定 : 組織が定めたデータ格納オブジェクト]</p> <p>データマイニングを適切に検出し、保護</p> <p>参照 : なし</p>	<p>AC-23</p> <p>[値は未設定。 CSP により設定される]</p>
<p>AT-1; 意識と訓練; セキュリティ意識と訓練の方針と手順 :</p> <p>組織 :</p> <p>a. 開発、文書化、配布</p>	<p>AT-1</p> <p>影響レベル 4-6 :</p> <p>a. すべての人員</p>

<p>〔設定：組織が定めた要員または役割〕：</p> <p>1. 目的、範囲、役割、責任、管理、コミットメント、組織間の調整、コンプライアンスを扱うセキュリティ意識と訓練の方針</p> <p>そして</p> <p>2. セキュリティ意識と訓練方針の徹底と関連事項を促進するための手順；</p> <p>そして</p> <p>b. 現状のレビューと更新：</p> <p>1. セキュリティ意識と訓練方針</p> <p>〔設定：組織が定めた頻度〕；</p> <p>そして</p> <p>2. セキュリティ意識と訓練手順</p> <p>〔設定：組織が定めた頻度〕</p> <p>参照：NIST Special Publications 800-12、800-16、800-50、800-100</p>	<p>根拠：</p> <p>DoD の RMF TAG</p> <p>-----</p> <p>すべての影響レベル：</p> <p>b. 1 少なくとも 3 年ごと</p> <p>b. 2 少なくとも毎年</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>AT-2；意識と訓練；セキュリティ意識</p> <p>RENAMED：セキュリティ意識啓発トレーニング：</p> <p>組織は、情報システムのユーザ（マネージャー、上級管理者、請負業者を含む）に基本的なセキュリティ意識啓発のトレーニングを提供</p> <p>a. 新規ユーザの初期トレーニングの一環として、</p> <p>b. 情報システムの変更が必要な場合。そして</p> <p>c. 〔設定：組織が定めた頻度〕</p> <p>その後、</p> <p>参照：C.F.R. パート 5 サブパート C（5 C.F.R. 930.301）；NIST Special Publication 800-50.</p>	<p>AT-2</p> <p>すべての影響レベル：</p> <p>c. 毎年</p> <p>根拠：</p> <p>DoD RMF TAG と FedRAMP v2</p> <p>-----</p>

<p>AT-3; 意識と訓練; セキュリティトレーニング RENAMED: 役割ベースのセキュリティトレーニング:</p> <p>組織は、割り当てられたセキュリティの役割と責任を持つ担当者にロールベースのセキュリティトレーニングを提供</p> <p>a. 情報システムへのアクセス許可や割り当てられた任務を実行する前に;</p> <p>b. 情報システムの変更が必要な場合。そして</p> <p>c. [設定: 組織が定めた頻度]</p> <p>その後.</p> <p>参照: C.F.R. パート 5 サブパート C (5 C.F.R. 930.301); NIST Special Publications 800-16、800-50.</p>	<p>AT-3</p> <p>すべての影響レベル:</p> <p>c. 毎年</p> <p>根拠:</p> <p>DoD RMF TAG と FedRAMP v2</p> <p>-----</p>
<p>AT-3 (2); 意識と訓練; セキュリティトレーニング RENAMED: 役割ベースのセキュリティトレーニング - 強化:</p> <p>物理的セキュリティ管理策</p> <p>組織の提供</p> <p>[設定: 組織が定めた要員または役割]</p> <p>最初および</p> <p>[設定: 組織が定めた頻度]</p> <p>雇用における訓練と物理的セキュリティ管理策の運用</p> <p>参照: なし</p>	<p>AT-3 (2)</p> <p>影響レベル 4-6:</p> <p>顧客の情報を含む媒体や CSO をサポートしてインフラを収容するスペースへ日常的な物理的アクセスの役割が割り当てられているすべての人員</p> <p>毎年</p> <p>根拠: DoD RMF TAG (商用 CSP の調整あり)</p> <p>-----</p>

<p>AT-3 (4) ; 意識と訓練; 役割に基づくセキュリティトレーニング - 強化 : 不審な通信と異常なシステム動作</p> <p>組織は、要員に対し訓練を提供</p> <p>[設定 : 組織が定めた悪質コードの指標]</p> <p>組織の情報システムにおける不審な通信や異常な振舞いの認識</p> <p>参照 : なし</p>	<p>AT-3 (4)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>AT-4; 意識と訓練; セキュリティトレーニングの記録 :</p> <p>組織 :</p> <p>a. 基本的なセキュリティ意識啓発訓練や特定の情報システムセキュリティ訓練を含む、要員の情報システムセキュリティ訓練活動を文書化しモニター そして</p> <p>b. 個々の訓練記録の保持</p> <p>[設定 : 組織が定めた期間]</p> <p>参照 : なし</p>	<p>AT-4</p> <p>影響レベル 4-6 :</p> <p>b. 最低 5 年または特定のトレーニングプログラムの完了後 5 年</p> <p>根拠 : DoD RMF TAG -----</p> <p>影響レベル 2 :</p> <p>少なくとも 1 年</p> <p>根拠 : FedRAMP v2 -----</p>
<p>AU-1; 監査と説明責任; 監査と説明責任の方針と手順 :</p> <p>組織 :</p> <p>a. 開発、文書化、配布</p> <p>[設定 : 組織が定めた要員または役割] :</p> <p>1. 目的、範囲、役割、責任、管理コミットメント、組織間の調整、コンプライアンスに対処する監査および説明責任ポリシー ;</p>	<p>AU-1</p> <p>影響レベル 4-6 :</p> <p>a. ISSO、ISSM、およびローカル組織が適切と考える他のもの</p> <p>b. 1. 毎年</p> <p>根拠 : DoD RMF TAG -----</p>

<p>2. 監査と説明責任の方針、および関連する監査の実施を促進する手順と説明責任コントロール；</p> <p>そして</p> <p>b. 現状のレビューと更新：</p> <p>1. 監査と説明責任ポリシー [設定：組織が定めた頻度]；</p> <p>2. 監査と説明責任手順 [設定：組織が定めた頻度].</p> <p>参照：NIST Special Publications 800-12、800-100.</p>	<p>影響レベル 2：</p> <p>b.1 少なくとも 3 年ごと</p> <p>根拠：FedRAMP v2</p> <p>すべての影響レベル：</p> <p>b.2 少なくとも年次</p> <p>根拠：DoD RMF TAG と FedRAMP v2</p> <p>-----</p>
<p>AU-2； 監査と説明責任； 監査対象イベント：</p> <p>組織：</p> <p>a. 情報システムが以下のイベントを監査できるかどうかを決定 [設定：組織が定めた監査可能な事象]；</p> <p>b. 監査関連の情報を必要とする他の組織とセキュリティ監査機能を調整し、相互サポートを強化して監査対象イベントの選択を手助け；</p> <p>c. 監査対象のイベントがセキュリティインシデントの事後調査をサポートするのに十分であると考えられる理由についての根拠を提供</p> <p>d. 情報システムの中で以下のイベントが監査されることを決定 [設定：組織が定めた監査イベント（サブセット AU-2 a.）で定義されている監査対象イベントの特定されたイベントそれぞれの監査の頻度（または必要な状況）]</p>	<p>AU-2</p> <p>影響レベル 4-6：</p> <p>a. 特権、セキュリティオブジェクト、セキュリティレベル、または情報のカテゴリ（分類レベルなど）のアクセス、変更、または削除の試行が成功したか失敗したか。特権アクティビティまたはその他のシステムレベルのアクセス、システムへのユーザーアクセスの開始および終了時間、異なるワークステーションからの同時ログオン、オブジェクトへの成功したアクセスおよび失敗したアクセス、すべてのプログラムの開始、情報システムへのすべての直接アクセス。すべてのアカウントの作成、変更、無効化、および終了。すべてのカーネルモジュールのロード、アンロード、再起動。</p> <p>d. AU-2 (a) で定義されたすべての監査対象事象</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>

<p>参照 : NIST Special Publication 800-92; Web : CSRC. NIST. GOV/PCIG/CIG. HTML, IDMANAGEMENT. GOV</p>	<p>影響レベル 2 :</p> <p>a. 成功したアカウントログオンイベント、アカウント管理イベント、オブジェクトアクセス、ポリシー変更、特権機能、プロセストラッキング、およびシステムイベント。Web アプリケーションの場合 : すべての管理者アクティビティ、認証チェック、権限チェック、データ削除、データアクセス、データ変更、および権限変更</p> <p>d. AU-2 a. で定義された監査可能なイベントの中で、組織が定めたサブセットについて識別されたイベントごとに継続的に監査</p> <p>根拠 : FedRAMP v2 -----</p>
<p>AU-2 (3) ; 監査と説明責任; 監査可能なイベント - 強化 : レビューと更新</p> <p>組織は、監査されたイベントのレビューの更新 [設定 : 組織が定めた頻度].</p> <p>参照 : なし</p>	<p>AU-2 (3)</p> <p>すべての影響レベル : 毎年および脅威、脆弱性の状況認識による。</p> <p>ソース : DoD RMF TAG と FedRAMP v2 -----</p> <p>FedRAMP 追加要件とガイダンス : ガイダンス : 毎年、または脅威環境の変化が公式機関からサービスプロバイダに伝えられる都度</p>
<p>AU-3 (1) ; 監査と説明責任; 監査記録の内容 - 強化 : 追加の監査情報</p> <p>情報システムは、以下を含む監査記録を生成</p>	<p>AU-3 (1)</p> <p>影響レベル 4-6 :</p>

<p>[設定：組織が定めた追加のより詳細な情報]</p> <p>参照：なし</p>	<p>少なくとも、特権コマンドまたはグループアカウントユーザの個々の ID のフルテキスト記録</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2：</p> <p>セッション、接続、トランザクション、またはアクティビティ期間； クライアント – サーバートランザクションの場合、受信バイト数と送信バイト数； イベントを診断または識別するための追加情報メッセージ； 操作されているオブジェクトまたはリソースを記述または識別する特性</p> <p>根拠：FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>AU-3 (1) . 要件：サービスプロバイダは、監査レコードタイプを定義。監査レコードタイプは承認当局で承認され受理される。</p> <p>ガイダンス：クライアントとサーバー間のトランザクションでは、送受信されるバイト数によって双方向の転送情報が得られ、調査や問い合わせの際に役立つ。</p>
<p>AU-4;監査と説明責任； 監査ストレージ容量：</p> <p>組織は、監査レコードの記憶容量を次により割り当てる。</p> <p>[設定：組織が定めた監査レコード記憶域要件]</p> <p>参照：なし</p>	<p>AU-4</p> <p>[値は未設定。 CSP により設定される]</p>

<p>AU-4 (1) ;監査と説明責任; 監査ストレージ容量-強化:</p> <p>代替ストレージへの転送</p> <p>情報システムは監査記録をオフロードする。</p> <p>[設定: 組織が定めた頻度]</p> <p>監査対象のシステムとは異なるシステムまたはメディアへ複写</p> <p>参照: なし</p>	<p>AU-4 (1)</p> <p>影響レベル 4-6:</p> <p>最低限、相互接続されたシステムの場合はリアルタイム、スタンドアロンシステムの場合は毎週</p> <p>根拠: DoD RMF TAG</p> <p>-----</p>
<p>AU-5; 監査と説明責任; 監査処理失敗への対応:</p> <p>情報システム:</p> <p>a. アラート</p> <p>[設定: 組織が定めた要員または役割]</p> <p>監査処理が失敗した場合、そして</p> <p>b. 次の追加アクションを実行</p> <p>[設定: 組織が定めた行動を実施 (例えば、情報システムをシャットダウンし、最も古い監査レコードを上書きし、監査レコードの生成を停止)]。</p> <p>参照: なし</p>	<p>AU-5</p> <p>影響レベル 4-6:</p> <p>a. 最低限、SCA と ISSO</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル:</p> <p>b. 影響の少ないもの: 最も古い監査レコードの上書き。中程度の影響: シャットダウン</p> <p>根拠: FedRAMP v2</p> <p>-----</p>
<p>AU-6; 監査と説明責任; 監査レビュー、分析と報告:</p> <p>組織:</p> <p>a. 情報システム監査記録のレビューと分析</p> <p>[設定: 組織が定めた頻度]</p> <p>兆候</p> <p>[設定: 組織が定めた不適切または異常なアクティビティ];</p>	<p>AU-6</p> <p>影響レベル 4-6:</p> <p>a. 7 日毎、またはアラームイベントや異常により必要とされる場合は、それ以上頻繁に</p>

<p>b. 調査結果の報告</p> <p>[設定：組織が定めた要員または役割]</p> <p>参照：なし</p>	<p>b. 少なくとも、ISSO と ISSM</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2：</p> <p>a. 少なくとも毎週</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>AU-7 (1)； 監査と説明責任； 監査の削減とレポートの生成 - 強化：</p> <p>自動処理</p> <p>情報システムは、以下に基づいて関心のあるイベントの監査記録を処理する能力を提供</p> <p>[設定：監査記録の中の組織が定めた監査フィールド]</p> <p>参照：なし</p>	<p>AU-7 (1)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>AU-8； 監査と説明責任； タイムスタンプ：</p> <p>情報システム：</p> <p>a. 監査記録のタイムスタンプを生成するために内部システムクロックを使用 そして</p> <p>b. 協定世界時 (UTC) またはグリニッジ標準時 (GMT) にマッピング可能な監査記録のタイムスタンプを記録し、次の要件を満たす。</p> <p>[設定：組織が定めた時間の詳細さで測定]</p> <p>参照：なし</p>	<p>AU-8</p> <p>影響レベル 4-6：</p> <p>b. 一秒</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>

<p>AU-8 (1) ; 監査と説明責任; 監査情報の保護</p> <p>- 強化 :</p> <p>信頼できる時刻ソースとの同期</p> <p>情報システム :</p> <p>a. 内部情報システムのクロックを比較</p> <p>[設定 : 組織が定めた頻度]</p> <p>次について</p> <p>[設定 : 組織が定めた正式な時刻ソース]</p> <p>そして</p> <p>b. 時差がより大きい場合、内部システムクロックを信頼できる時刻ソースに同期させる。</p> <p>[設定 : 組織が定めた期間].</p> <p>参照 : なし</p>	<p>AU-8 (1)</p> <p>影響レベル 4-6 :</p> <p>a. 適切な DoD ネットワーク (NIPRNet/ SIPRNet) や全地球測位システム (GPS) のために指定された代替米国海軍天文台 (USNO) の時刻サーバーと同期した信頼できる時刻サーバー</p> <p>b. AU-8 の組織的に定義された粒度より大きい。</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル :</p> <p>a. 少なくとも毎時</p> <p>根拠 : FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス :</p> <p>AU-8 (1) . 要件 : サービスプロバイダは、NIST インターネット時刻サービスで使用するプライマリとセカンダリの時刻サーバーを選択する。セカンダリサーバは、プライマリサーバとは異なる地域から選択される。</p> <p>要件 : サービスプロバイダは、Windows 以外のオペレーティングシステムを実行するネットワークコンピュータのシステムクロックを Windows Server ドメインコントローラエミュレータまたはそのサーバーの同じ時刻ソースに同期させる。</p> <p>ガイダンス : システムクロックの同期は、ログ解析の精度向上に寄与</p>
--	---

<p>AU-9 (2) ; 監査と説明責任; 監査情報の保護 - 強化 : 個別の物理システム/コンポーネントでの監査 バックアップ</p> <p>情報システムにおける監査レコードのバック アップ</p> <p>[設定 : 組織が定めた頻度]</p> <p>監査対象のシステムやコンポーネントとは物 理的に異なるシステムまたはシステムコンポ ーネントへ</p> <p>参照 : なし</p>	<p>AU-9 (2)</p> <p>すべての影響レベル : 少なくとも毎週</p> <p>根拠 : DoD RMF TAG&FedRAMP v2 -----</p>
<p>AU-9 (4) ; 監査と説明責任; 監査情報の保護 - 強化 : 特権ユーザのサブセットによるアクセス</p> <p>組織は、監査機能の管理へのアクセスのみを 許可</p> <p>[設定 : 組織が定めた特権ユーザのサブセッ ト].</p> <p>参照 : なし</p>	<p>AU-9 (4)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>AU-11; 監査と説明責任; 監査レコード保持期 間 :</p> <p>組織は、</p> <p>[設定 : 記録保存ポリシーに沿って組織が定 めた期間]</p> <p>セキュリティインシデントの事後調査を支援 し、規制上や組織上の情報保持要件を満たす ことができる。</p> <p>参照 : なし</p>	<p>AU-11</p> <p>影響レベル 4-6 : SAMI では 5 年; それ以外の場合は少なく とも 1 年</p> <p>根拠 : DoD RMF TAG -----</p> <p>影響レベル 2 : 少なくとも 90 日 根拠 : FedRAMP v2 -----</p>

	<p>FedRAMP 追加要件とガイダンス：</p> <p>AU-11. 要件：サービスプロバイダは、少なくとも 90 日間オンラインで監査記録を保持し、NARA 要件に準拠する期間、監査記録をオフラインで保存</p> <p>NARA の一般的な記録スケジュール http://www.archives.gov/records-mgmt/grs.html</p>
<p>AU-12； 監査と説明責任； 監査の生成：</p> <p>情報システム：</p> <p>a. AU-2 a. で定義された監査可能なイベントの監査レコード生成機能を提供</p> <p>〔設定：組織が定めた情報システムコンポーネント〕；</p> <p>b. 許可</p> <p>〔設定：組織が定めた要員または役割〕</p> <p>情報システムの特定のコンポーネントによって監査される監査対象イベントを選択 そして</p> <p>c. AU-3 で定義されている内容で、AU-2 で定義されたイベントの監査レコードを生成</p> <p>参照：なし</p>	<p>AU-12</p> <p>影響レベル 4-6：</p> <p>a. すべての情報システムとネットワークコンポーネント</p> <p>b. ISSM または ISSM によって任命された要員</p> <p>根拠：DoD RMF TAG -----</p> <p>影響レベル 2：</p> <p>a. 監査機能の導入や使用可能なすべての情報システムおよびネットワークコンポーネント</p> <p>根拠：FedRAMP v2 -----</p>
<p>AU-12 (1)； 監査と説明責任； 監査の生成 - 強化：</p> <p>システム全体/時刻相関の監査証跡</p>	<p>AU-12 (1)</p> <p>影響レベル 4-6：</p> <p>AU-8 で定義された時刻追跡許容誤差</p>

<p>情報システムは、</p> <p>〔設定：組織が定めた情報システムコンポーネント〕</p> <p>システム全体に渡る（論理的または物理的な）監査証跡に変換</p> <p>〔設定：監査証跡の中の個々の記録のタイムスタンプの関係に対する組織が定めた許容レベル〕</p> <p>参照：なし</p>	<p>根拠：DoD RMF TAG</p> <p>-----</p>
<p>CA-1；セキュリティアセスメントと認証；セキュリティアセスメントと承認ポリシー及び手順：</p> <p>組織：</p> <p>a. 開発、文書化、配布</p> <p>〔設定：組織が定めた要員または役割〕：</p> <p>1. セキュリティアセスメントおよび権限付与とポリシー、目的、範囲、役割、責任、経営者のコミットメント、組織間の調整、コンプライアンス そして</p> <p>2. セキュリティアセスメントと認可ポリシーの実施を促進するための手続および関連するセキュリティアセスメントおよび権限管理</p> <p>そして</p> <p>b. 現状のレビューと更新：</p> <p>1. セキュリティアセスメントと承認ポリシー</p> <p>〔設定：組織が定めた頻度〕</p> <p>そして</p> <p>2. セキュリティアセスメントと承認手順</p> <p>〔設定：組織が定めた頻度〕</p>	<p>CA-1</p> <p>影響レベル 4-6：</p> <p>a. すべての要員</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル：</p> <p>b. 1 少なくとも 3 年ごと</p> <p>b. 2 少なくとも毎年</p> <p>根拠：FedRAMP v2</p> <p>-----</p>

参照：NIST Special Publications 800-12、800-37、800-53A、800-100.	
<p>CA-2;セキュリティアセスメントと認証;セキュリティアセスメント:</p> <p>組織:</p> <p>a. 次のような評価の範囲を説明するセキュリティアセスメント計画を作成</p> <ol style="list-style-type: none">1. 評価中のセキュリティ管理策とコントロール強化:2. セキュリティ管理策の有効性を判断するために使用される評価手順。そして3. 評価環境、評価チーム、および評価の役割と責任 <p>b. 情報システムとその運用環境におけるセキュリティ管理策の評価</p> <p>[設定：組織が定めた頻度]</p> <p>どのコントロールが正しく実装され、意図したように運用され、確立されたセキュリティ要件を満たすことに関して所望した結果を生み出しているかを決定</p> <p>c. アセスメント結果を文書化し、セキュリティアセスメントレポートを作成</p> <p>d. セキュリティ管理策評価の結果を</p> <p>[設定：組織が定めた個人または役割].</p> <p>参照：大統領令 12587; FIPS Publication 199; NIST Special Publications 800-37, 800-39, 800-53A、800-115、800-137</p>	<p>CA-2</p> <p>すべての影響レベル:</p> <p>b. 少なくとも年に 1 回</p> <p>根拠：FedRAMP v2</p> <p>-----</p> <p>d. 最低限、CSP の ISSO と ISSM、FedRAMP PMO (該当する場合)、DISA A&A/SCA チーム、および顧客の MCD</p> <p>根拠：商用と DoD プライベートオンプレミス CSP/CSO を考慮した FedRAMP v2、DoD RMF TAG</p> <p>-----</p>
<p>CA-2 (1) ; セキュリティアセスメントと認証; セキュリティアセスメント - 強化:</p> <p>独立した評価者</p> <p>組織は、</p> <p>[設定：組織が定めた独立性]</p>	<p>CA-2 (1)</p> <p>すべての影響レベル:</p> <p>NIST Baseline へ低 FedRAM として追加</p> <p>根拠：FedRAMP v2</p> <p>-----</p>

セキュリティ管理策のアセスメントの実施 参照：なし	FedRAMP 追加要件とガイダンス： JAB 認定の場合、認定 3PA0 であること
CA-2 (2) ; セキュリティアセスメントと 証；セキュリティアセスメント - 強化： 専門的な評価 組織は、セキュリティ管理策アセスメントの 一環として、 [設定：組織が定めた頻度]， [選択： - 公表； - 非公表]， [選択 (1 つまたは複数)： - 詳細な監視； - 脆弱性スキャン； - 悪意のあるユーザのテスト； - インサイダー脅威評価； - パフォーマンス/負荷テスト； - [設定：組織が定めた他の形態のセキュ リティ評価]]。 参照：なし	CA-2 (2) すべての影響レベル： 少なくとも年に 1 回 根拠：FedRAMP v2 ----- FedRAMP 追加要件とガイダンス： 要件：「公表」、「脆弱性スキャン」を含む
CA-2 (3) ; セキュリティアセスメントと 証；セキュリティアセスメント - 強化： 外部組織 組織は、以下のアセスメント結果を受け入れ る。 [設定：組織が定めた情報システム] 次により実行された	CA-2 (3) すべての影響レベル： CSP および CSO インフラ 任意の FedRAMP 認定 3PA0 FedRAMP リポジトリ内の PA の条件

<p>[設定：組織が定めた外部組織]</p> <p>アセスメントが満たされたとき</p> <p>[設定：組織が定めた要件]</p> <p>参照：なし</p>	<p>根拠：FedRAMP v2</p> <p>-----</p>
<p>CA-3；セキュリティアセスメントと認証；情報システムの接続 RENAMED：システムの相互接続：</p> <p>組織：</p> <p>a. 相互接続セキュリティ規約により、情報システムから他の情報システムへの接続認可</p> <p>b. 各相互接続、インターフェース特性、セキュリティ要件、および伝達される情報の性質に関する文書。そして</p> <p>c. 相互接続セキュリティ規約のレビューと更新</p> <p>[設定：組織が定めた頻度]</p> <p>参照：FIPS Publication 199；NIST Special Publication 800-47</p>	<p>CA-3</p> <p>すべての影響レベル：</p> <p>c. 少なくとも年に1回</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>影響レベル2：</p> <p>c. 3年/年次およびFedRAMPからのインプット</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>CA-3 (1)；セキュリティアセスメントと認証；情報システムの接続 RENAMED：システムの相互接続 - 強化：</p> <p>非格付けの国家セキュリティシステム接続</p> <p>組織は、</p> <p>[設定：組織が格付けしていない、国家セキュリティシステム]</p> <p>次を使用しない外部ネットワークに接続</p> <p>[設定：組織が定めた境界保護デバイス]</p> <p>参照：なし</p>	<p>CA-3 (1)</p> <p>影響レベル4-6：</p> <p>すべての非格付けのNSS</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>

<p>CA-3 (3) ; セキュリティアセスメントと認証; システム相互接続 - 強化: 非格付けの非国家セキュリティシステム接続</p> <p>組織は、</p> <p>[設定: 組織が定義していない、非国家セキュリティシステム]</p> <p>次を使用しない外部ネットワークに接続</p> <p>[設定: 組織が定めた境界保護デバイス]</p> <p>参照: なし</p>	<p>CA-3 (3)</p> <p>すべての影響レベル:</p> <p>信頼できるインターネット接続 (TIC) 要件を満たす境界保護</p> <p>根拠: FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス: CA-3 (3) ガイダンス: 付録 H 「TIC 2.0 リファレンスアーキテクチャ」ドキュメントの「クラウドに関する考慮事項」を参照 https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf</p>
<p>CA-3 (5) ; セキュリティアセスメントと認証; システム相互接続 - 強化: 外部システム接続の制限事項</p> <p>組織は、</p> <p>[選択:</p> <ul style="list-style-type: none">- すべて許可;- 例外による拒否;- すべて否定;- 例外による許可 <p>]</p> <p>許可するためのポリシー</p> <p>[設定: 組織が定めた情報システム] 外部の情報システムへ接続</p> <p>参照: なし</p>	<p>CA-3 (5)</p> <p>影響レベル 4-6:</p> <p>拒否、例外による許可</p> <p>外部接続を必要とするシステム</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル:</p> <p>FedRAMP 追加要件とガイダンス: JAB 認可の場合、CSP は、このコントロールの詳細をアーキテクチャブリーフィングに含めなければならない。</p>

<p>CA-5; セキュリティアセスメントと認証; アクションプランとマイルストーンの計画:</p> <p>組織:</p> <p>a. セキュリティ管理策のアセスメント中に指摘された弱点や欠点を修正し、システムの既知の脆弱性を削減または排除し、組織により計画された是正措置を文書化するための情報システムのアクションプランとマイルストーンの策定 そして</p> <p>b. 既存のアクションプランとマイルストーンを更新</p> <p>[設定: 組織が定めた頻度]</p> <p>セキュリティ管理策アセスメント、セキュリティ影響分析や継続的な監視アクティビティから得られた知見に基づく。</p> <p>参照: OMB 覚書 02-01; NIST Special Publication 800-37</p>	<p>CA-5</p> <p>すべての影響レベル:</p> <p>b. 少なくとも毎月</p> <p>根拠: FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス:</p> <p>CA-5 ガイダンス: 要件: POA&M は、少なくとも月に一回実行されること。</p>
<p>CA-6; セキュリティアセスメントと認証; セキュリティ認証:</p> <p>組織:</p> <p>a. 情報システムの認証担当官として、上級レベルの幹部またはマネージャーを割り当てる。</p> <p>b. 情報システムによる処理の運用開始の前に、公式な認証を確実に得る。そして</p> <p>c. セキュリティ認証の更新</p> <p>[設定: 組織が定めた頻度]</p> <p>参照: OMB Circular A-130; OMB 覚書 11-33; NIST Special Publication 800-37、800-137</p>	<p>CA-6</p> <p>影響レベル 4-6:</p> <p>c. システムに重大な変更がある場合、またはシステムが動作する環境が変更された場合は、少なくとも 3 年ごとに更新</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2:</p> <p>c. 少なくとも 3 年ごとまたは大幅な変更が発生した場合</p> <p>根拠: FedRAMP v2</p> <p>-----</p>

	<p>FedRAMP 追加要件とガイダンス：</p> <p>CA-6c. ガイダンス：重要な変更は、NIST Special Publication 800-37 改訂第1版、付録Fに定義されている。サービスプロバイダは、リスクの様態に影響を与える情報システムまたは運用環境への変更のタイプを記述する。変更内容は承認担当官による承認を得て受理される。</p>
<p>CA-7;セキュリティアセスメントと認証;継続的モニタリング：</p> <p>組織は継続的なモニタリング戦略を策定し、以下を含む継続的なモニタリングプログラムを実施</p> <p>a. 策定 [設定：組織が定めた指標] 監視される；</p> <p>b. 策定 [設定：組織が定めた頻度] 監視と [設定：組織が定めた頻度] モニタリングを支援するアセスメントのために；</p> <p>c. 組織の継続的なモニタリング戦略に沿ったセキュリティ管理策アセスメント</p> <p>d. 組織の継続的なモニタリング戦略に沿って、組織が定めた指標による継続的なセキュリティ状態のモニタリング</p> <p>e. アセスメントとモニタリングによって生成されたセキュリティ関連情報の相関と分析</p> <p>f. セキュリティ関連情報の分析結果に対処するための対処アクション そして</p> <p>g. 組織における情報システムのセキュリティ状態の報告 [設定：組織が定めた要員または役割]</p>	<p>CA-7</p> <p>すべての影響レベル：</p> <p>d. 連邦およびFedRAMP の要件を満たすため</p> <p>根拠：FedRAMP v2 -----</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>オペレーティングシステムスキャン：少なくとも毎月</p> <p>データベースと Web アプリケーションのスキャン：少なくとも毎月</p> <p>独立した監査員が行う全スキャン：少なくとも年1回</p> <p>CA-7 ガイダンス：CSP は、標準的な POA&M アップデートの期間内に高い脆弱性の除去や修復の証拠を提出しなければならない。</p> <p>注： 'd' にはパラメータがなく、パラメータ値の 'd' のリストに矛盾がある。しかし、これは FedRAMP v2 のパラメータ定義そのものである。</p>

<p>[設定：組織が定めた頻度].</p> <p>参照：OMG メモ 11-33. NIST Special Publications 800-37 800-39、800-53A、800-115、800-137; US-CERT テクニカルサイバーセキュリティアラート; DoD 情報保証脆弱性アラート</p>	
<p>CA-7 (1) ; セキュリティアセスメントと認証; 継続的なモニタリング - 強化: 独立したアセスメント</p> <p>組織は、</p> <p>[設定：組織が定めた独立性]</p> <p>情報システムのセキュリティ管理策を継続的に監視</p> <p>参照：なし</p>	<p>CA-7 (1)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>CA-8; セキュリティアセスメントと認証; 侵入テスト:</p> <p>組織は侵入テストを実施</p> <p>[設定：組織が定めた頻度]</p> <p>次について</p> <p>[設定：組織が定めた情報システムまたはシステム構成要素].</p> <p>参照：なし</p>	<p>CA-8</p> <p>すべての影響レベル:</p> <p>少なくとも年に 1 回</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>CA-9; セキュリティアセスメントと認証; 内部システム接続:</p> <p>組織:</p> <p>a. 内部接続を許可する。</p> <p>[設定：組織が定めた情報システムコンポーネントまたはコンポーネントのクラス]</p>	<p>CA-9</p> <p>[値は未設定。 CSP により設定される]</p>

<p>情報システムに対し そして</p> <p>b. 各内部接続、インターフェース特性、セキュリティ要件や伝達される情報の性質に関する文書</p> <p>参照：なし</p>	
<p>CM-1; ベースライン・コンフィグレーション; 構成管理のポリシーと手順:</p> <p>組織:</p> <p>a. 作成、文書化、配布</p> <p>[設定: 組織が定めた要員または役割]:</p> <p>1. 目的、範囲、役割、責任、管理を扱う構成管理ポリシー</p> <p>コミットメント、組織間の調整、コンプライアンス</p> <p>そして</p> <p>2. 構成管理ポリシーの実装を容易にするための手順と、構成管理コントロール。</p> <p>そして</p> <p>b. 現状のレビューと更新:</p> <p>1. 構成管理ポリシー</p> <p>[設定: 組織が定めた頻度].</p> <p>そして</p> <p>2. 構成管理手順</p> <p>[設定: 組織が定めた頻度].</p> <p>参照: NIST Special Publications 800-12、800-100</p>	<p>CM-1</p> <p>影響レベル 4-6:</p> <p>a. 構成管理プロセスのすべての関係者</p> <p>b. 1. 毎年</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2:</p> <p>b. 1. 少なくとも 3 年ごと</p> <p>すべての影響レベル:</p> <p>b. 2. 少なくとも年に 1 回</p> <p>根拠: FedRAMP v2</p> <p>-----</p>
<p>CM-2 (1) ;ベースライン・コンフィグレーション; ベースライン設定 - 強化: レビューと更新</p> <p>組織は、情報システムのベースライン構成を見直し、更新</p>	<p>CM-2 (1)</p> <p>すべての影響レベル:</p> <p>a. 少なくとも 1 年ごと</p> <p>影響レベル 4-6:</p>

<p>a. [設定：組織が定めた頻度]；</p> <p>b. 必要な場合</p> <p>[設定：組織が定めた状況]；</p> <p>そして</p> <p>c. 情報システムコンポーネントのインストールやアップグレードの不可欠な部分</p> <p>参照：なし</p>	<p>c. ベースライン形態の変更、または USCYBERCOM 技術指令/指示やサイバー攻撃などの事象</p> <p>根拠： DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2：</p> <p>b. 認可担当官の指示を含む。</p> <p>根拠： FedRAMP v2</p> <p>-----</p>
<p>CM-2 (3) ； ベースライン・形態； ベースライン設定 - 強化：</p> <p>以前の構成の保持</p> <p>組織は保持</p> <p>[設定：組織が定めた以前のバージョンの情報システムのベースライン構成]</p> <p>ロールバックをサポート</p> <p>参照：なし</p>	<p>CM-2 (3)</p> <p>影響レベル 4-6：</p> <p>IS コンポーネントの前回承認されたベースライン構成は最低 3 ヶ月間</p> <p>根拠： DoD RMF TAG</p> <p>-----</p>
<p>CM-2 (7) ； 形態管理； ベースライン設定 - 強化：</p> <p>リスクが高い分野向けのシステム、コンポーネント、またはデバイスの設定</p> <p>組織：</p> <p>a. 発出</p> <p>[設定：組織が定めた情報システム、システムコンポーネント、またはデバイス]</p> <p>次について</p> <p>[設定：組織が定めた構成]</p> <p>組織が重大なリスクを有すると考える場所へ旅行する個人に、そして</p> <p>b. 適用</p>	<p>CM-2 (7)</p> <p>[値は未設定。 CSP により設定される]</p>

<p>[設定：組織が定めたセキュリティ保護手段]</p> <p>個人が戻ったときにデバイスに対して</p> <p>参照：なし</p>	
<p>CM-3； ベースライン形態;形態変更管理：</p> <p>組織：</p> <p>a. 形態管理されている情報システムへの変更のタイプを決定</p> <p>b. 情報システムに対する形態変更の提案をレビューし、明示的なセキュリティ影響分析の結果に基づいて、変更を承認または拒否</p> <p>c. 情報システムに対する形態の変更決定を文書化</p> <p>d. 情報システムに対する承認された形態コントロールの変更を実装</p> <p>e. 情報システムに対する形態変更の記録を保持</p> <p>[設定：組織が定めた期間]；</p> <p>f. 情報システムの形態変更に関連するアクティビティの監査とレビュー そして</p> <p>g. 次により、形態変更の管理活動を調整、監視</p> <p>[設定：組織が定めた形態変更コントロール組織（例えば、委員会、理事会）]</p> <p>召集</p> <p>[選択（1 つまたは複数）：</p> <ul style="list-style-type: none"> - [設定：組織が定めた頻度] - [設定：組織が定めた構成, 変更の状態] <p>].</p> <p>参照：NIST Special Publication 800-128</p>	<p>CM-3</p> <p>影響レベル 4-6：</p> <p>e. 期間については、組織の CCB で定義する必要がある。</p> <p>g. コンフィグレーションコントロールボード</p> <p>g. CCB によって決定された頻度</p> <p>g. CCB によって決定される形態変更条件</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル：</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>要件：サービスプロバイダは、連邦政府と関連するサービス利用（例えば、電子掲示板、ウェブステータスページ）へ影響する可能性のある情報システムまたは運用環境における主要な変更または開発を伝える一元的な手段を確立する。コミュニケーションの手段は、認可担当官の承認を受ける。</p> <p>CM-3e ガイダンス：記録保存の方針と手順に従う。</p>

<p>CM-3 (4) ; ベースライン形態;形態変更管理の強化 :</p> <p>セキュリティ担当者</p> <p>組織には、次のメンバーとなるセキュリティ代表者が必要</p> <p>[設定 : 組織が定めた形態変更コントロール組織]</p> <p>参照 : なし</p>	<p>CM-3 (4)</p> <p>影響レベル 4-6 :</p> <p>コンフィギュレーション・コントロール・ボード (CCB) (CM-3, CCI 1586 で定義)</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p>
<p>CM-3 (6) ; 形態管理; 形態変更管理の強化 : 暗号管理</p> <p>組織は、暗号メカニズムの使用で次を保証</p> <p>[設定 : 組織が定めたセキュリティ保護手段]</p> <p>形態管理下にある</p> <p>参照 : なし</p>	<p>CM-3 (6)</p> <p>影響レベル 4-6 :</p> <p>暗号化に依存するすべてのセキュリティ保護</p> <p>根拠 : DoD RMF TAG&CNSSI 1253</p>
<p>CM-5 (3) ; 変更のアクセス制限 - 強化 : 署名されたコンポーネント</p> <p>情報システムは、の検証なしに次の導入を防止</p> <p>[設定 : 組織が定めた重要なソフトウェアとファームウェアコンポーネント]</p> <p>コンポーネントが組織によって認識・承認された証明書によるデジタル署名</p> <p>参照 : なし</p>	<p>CM-5 (3)</p> <p>影響レベル 4-6 :</p> <p>ベンダーがデジタル署名された製品を提供する場合のソフトウェアやファームウェアコンポーネント</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル :</p> <p>FedRAMP 追加要件とガイダンス :</p> <p>ガイダンス : デジタル署名/証明書が利用できない場合は、代替の完全性チェック (ハッシュ、自己署名証明書など) を利用できる。</p>

<p>CM-5 (5) ; ベースライン・コンフィグレーション; 変更のアクセス制限 - 強化: 製造/運用中の特権の制限</p> <p>組織:</p> <p>a. 製造中および運用環境内の情報システムコンポーネントやシステム関連の情報を変更する権限を制限—そして</p> <p>b. 特権をレビューし再評価 [設定: 組織が定めた頻度]</p> <p>参照: なし</p>	<p>CM-5 (5)</p> <p>すべての影響レベル:</p> <p>b. 少なくとも四半期ごと</p> <p>根拠: FedRAMP v2 -----</p>
<p>CM-6; ベースライン・コンフィグレーション; 構成設定:</p> <p>組織:</p> <p>a. 情報システム内で使用される情報技術製品の構成設定を確立し、文書化 [設定: 組織が定めたセキュリティ構成チェックリスト]</p> <p>運用上の要求に合致する最も制限的なモードを反映した</p> <p>b. 構成の設定を実装</p> <p>c. 確立された構成設定からの逸脱を識別、文書化、承認 [設定: 組織が定めた情報システムコンポーネント]</p> <p>次に基づく [設定: 組織が定めた運用要件]; そして</p> <p>d. 組織のポリシーおよび手順に従って、形態設定の変更を監視しコントロール</p>	<p>CM-6</p> <p>影響レベル 4-6:</p> <p>a. DoD セキュリティコンフィグレーションまたは実装ガイド (STIG、SRG、NSA コンフィグレーションガイド、CTO、DTM など)</p> <p>c. すべての設定可能な情報システムコンポーネント</p> <p>根拠: DoD RMF TAG</p> <p>注: DISA は、商用 CSP の同等性をケースバイケースで評価。そのような同等性の例として、CIS のベンチマークを利用できる。 -----</p> <p>影響レベル 2:</p> <p>a. CM-6 (a) 追加の FedRAMP 要件およびガイダンスを参照</p> <p>根拠: FedRAMP v2 -----</p>

<p>参照：OMB メモ 07-11、07-18、08-22； NIST Special Publications 800-70、800-128； Web：nvd.nist.gov； checklists.nist.gov； www.nsa.gov</p>	<p>FedRAMP 追加要件とガイダンス： CM-6a. 要件：サービスプロバイダは、USGCB が利用できない場合、インターネットセキュリティセンターのガイドライン（レベル 1）を使用して形態設定を確立し、独自の形態設定を確立しなければならない。 CM-6a. 要件：サービスプロバイダは、構成設定のチェックリストが SCAP（Security Content Automation Protocol）または SCAP と互換性があることを確認しなければならない（検証済みのチェックリストが利用できない場合）。 CM-6a. ガイダンス：USGCB のチェックリストに関する情報は次を参照 http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc</p>
<p>CM-6（1）； ベースライン・コンフィグレーション； 構成設定 - 強化： 自動一元管理/アプリケーション/検証</p> <p>組織は、自動設定されたメカニズムを使用して、形態の設定を一元的に管理、適用、検証 [設定：組織が定めた情報システムコンポーネント]</p> <p>参照：なし</p>	<p>CM-6（1）</p> <p>[値は未設定。 CSP により設定される]</p>
<p>CM-7； ベースライン・コンフィグレーション； 最低限の機能性：</p> <p>組織：</p> <p>a. 必要最小限な機能のみを提供するように情報システムを構成—そして</p> <p>b. 機能、ポート、プロトコルやサービスの使用を禁止または制限</p>	<p>CM-7</p> <p>影響レベル 4-6： DoD 8551.01 に従って</p> <p>根拠：DoD RMF TAG -----</p>

<p>[設定：組織が定めた禁止または制限された機能ポート、プロトコルやサービス]</p> <p>参照：DoD の指示 8551.01</p>	<p>影響レベル 2：</p> <p>米国政府構成ベースライン (USGCB)</p> <p>根拠：FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>要件：サービスプロバイダは、禁止または制限された機能、ポート、プロトコルやサービスのリストを確立するために、インターネットセキュリティセンターのガイドライン（レベル 1）を使用するか、または USGCB が利用できない場合は、独自のリストを作成しなければならない。</p> <p>CM-7. ガイダンス：USGCB のチェックリストに関する情報は、次を参照 http://usgcb.nist.gov/usgcb_faq.html#usgcbfaq_usgcbfdcc</p> <p>（部分的に AC-17(8). に由来）</p>
<p>CM-7 (1)；ベースライン・コンフィグレーション；最低限の機能 - 強化：</p> <p>定期的レビュー</p> <p>組織：</p> <p>a. 情報システムのレビュー</p> <p>[設定：組織が定めた頻度]</p> <p>不要な機能や安全ではない機能、ポート、プロトコル、およびサービスを識別—そして</p> <p>b. 無効化</p> <p>[設定：組織が定めた、情報システム内で不要・安全でないとみなされるサービス機能、ポート、プロトコル]</p> <p>参照：なし</p>	<p>CM-7 (1)</p> <p>すべての影響レベル：</p> <p>a. 少なくとも毎月</p> <p>根拠：FedRAMP v2</p> <p>-----</p> <p>影響レベル 4-6：</p> <p>b. 安全でない機能、ポート、プロトコルやサービスは、DoD 8551.01 で定義されている。</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>

<p>CM-7 (2) ; ベースライン・コンフィグレーション; 最低限の機能 - 強化: プログラムの実行防止</p> <p>情報システムは、次に従ってプログラムの実行を防止</p> <p>[選択 (1 つまたは複数):</p> <ul style="list-style-type: none">- [設定: ソフトウェア・プログラムの使用と制限にし、組織が定めたポリシー];- ソフトウェア・プログラム使用の条件を認可するルール <p>]</p> <p>参照: なし</p>	<p>CM-7 (2)</p> <p>すべての影響レベル:</p> <p>FedRAMP 追加要件とガイダンス:</p> <p>CM-7 (2) ガイダンス: このコントロールは、情報システム上で技術的な方法で実施され、ポリシーに従ったプログラム (すなわちホワイトリスト) のみを実行できるようにするものとする。このコントロールは、実行が許可されているかどうかに関する厳密に書かれたポリシーに基づいて行われるものではない。</p>
<p>CM-7 (5) ; コンフィグレーション管理; 最低限の機能 - 強化: 認定ソフトウェア/ホワイトリスト</p> <p>組織:</p> <p>a. 識別する</p> <p>[設定: 情報システム上で実行する許可を得た組織が定めたソフトウェア・プログラム]</p> <p>b. 情報システム上で許可されたソフトウェア・プログラムの実行を許可するために、「全て拒否、許可は例外ポリシー」を採用 - そして</p> <p>c. 承認されたソフトウェア・プログラムのリストをレビューし、更新</p> <p>[設定: 組織が定めた頻度]。</p> <p>参照: なし</p>	<p>CM-7 (5)</p> <p>影響レベル 4-6:</p> <p>c. 毎月</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2:</p> <p>c. 少なくとも年に 1 回、または変更があるとき。</p> <p>根拠: FedRAMP v2</p> <p>-----</p>

<p>CM-8; ベースライン・コンフィグレーション; 情報システムコンポーネントインベントリ :</p> <p>組織 :</p> <p>a. 情報システムコンポーネントの品目一覧を 文書化</p> <ol style="list-style-type: none">1. 現在の情報システムを正確に反映2. 情報システムの認可境界内のすべてのコン ポーネントを含む。3. 追跡や報告に必要とされる粒度レベルで4. 以下を含む。 <p>[設定 : 効果的な情報システムの達成に必 要と見なされるコンポーネントのアカウ ンタビリティ]; そして</p> <p>b. 情報システムコンポーネント品目一覧のレ ビューと更新</p> <p>[設定 : 組織が定めた頻度]。</p> <p>参照 : NIST Special Publication 800-128</p>	<p>CM-8</p> <p>影響レベル 4-6 :</p> <p>a. ハードウェアインベントリ仕様 (製造 元、タイプ、モデル、シリアル番号、物理 的な場所)、ソフトウェアライセンス情 報、情報システム/コンポーネント所有 者、ネットワークコンポーネント/デバイ スのマシン名</p> <p>根拠 : DoD RMF TAG -----</p> <p>すべての影響レベル :</p> <p>b. 少なくとも毎月</p> <p>根拠 : FedRAMP v2 -----</p> <p>FedRAMP 追加要件とガイダンス :</p> <p>CM-8 要件 : 少なくとも月に一度、または 変更があった場合に提供</p>
<p>CM-8 (3) ; ベースライン・コンフィグレーシ ョン; 情報システムコンポーネントインベン トリ - 強化 :</p> <p>自動化された不正なコンポーネントの検出</p> <p>組織 :</p> <p>a. 情報システム内の許可されていないハード ウェア、ソフトウェア、およびファームウェ アコンポーネントの存在を検出するための自 動メカニズム [設定 : 組織が定めた頻度] を採 用 —そして</p>	<p>CM-8 (3)</p> <p>影響レベル 4-6 :</p> <p>b. ISSO、ISSM、その他、現場の組織が適 切と判断したもの</p> <p>根拠 : DoD RMF TAG -----</p> <p>すべての影響レベル :</p>

<p>b. 許可されていないコンポーネントが検出された場合</p> <p>[選択 (1 つまたは複数) :</p> <ul style="list-style-type: none">- そのようなコンポーネントによるネットワークアクセスを無効化- コンポーネントの分離- [設定 : 組織が定めた要員または役割] <p>]</p> <p>参照 : なし</p>	<p>a. 検出までの遅延が最大 5 分である、自動化されたメカニズムを使用して、継続的に</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>
<p>CM-10 (1) ; コンフィグレーション管理; ソフトウェア使用制限 - 強化 : オープンソースソフトウェア</p> <p>組織は、オープンソースソフトウェアの使用に関して次の制限を設ける</p> <p>[設定 : 組織が定める制限事項]。</p> <p>参照 : なし</p>	<p>CM-10 (1)</p> <p>影響レベル 4-6 :</p> <p>DoD メモ「オープンソースソフトウェア (OSS) に関するガイダンスの明確化」による。2009 年 10 月 16 日 (http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf)</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p>
<p>CM-11; コンフィグレーション管理; ユーザがインストールしたソフトウェア :</p> <p>組織 :</p> <p>a. 確立する</p> <p>[設定 : 組織が定めた方針];</p> <p>ユーザによるソフトウェアのインストールを管理</p> <p>b. ソフトウェアのインストールポリシー</p> <p>[設定 : 組織が定めた方法];</p> <p>そして</p> <p>c. ポリシーのコンプライアンスを監視する</p> <p>[設定 : 組織が定めた頻度];</p> <p>参照 : なし</p>	<p>CM-11</p> <p>すべての影響レベル :</p> <p>c. 継続的に (CM-7 (5) 経由で)</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>

<p>CP-1; 緊急事態対応計画; 緊急事態対応計画の方針と手順:</p> <p>組織:</p> <p>a. 作成、文書化、配布</p> <p>[設定: 組織が定めた要員または役割]:</p> <ol style="list-style-type: none"> 1. 目的、範囲、役割、責任、管理を扱う緊急事態対応計画ポリシー、コミットメント、組織間の調整、コンプライアンスそして 2. 緊急時対応計画の実施を促進するための手順、不測の事態の計画策定 <p>そして</p> <p>b. 現状のレビューと更新:</p> <ol style="list-style-type: none"> 1. 緊急時計画の方針 <p>[設定: 組織が定めた頻度];</p> <p>そして</p> <ol style="list-style-type: none"> 2. 緊急時の計画手続き <p>[設定: 組織が定めた頻度];</p> <p>参照: 連邦事業継続指令 1。 NIST Special Publications 800-12, 800-34, 800-100.</p>	<p>CP-1</p> <p>影響レベル 4-6:</p> <p>a. 緊急時対応計画で特定されたすべてのステークホルダー</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル:</p> <p>b.1 少なくとも 3 年ごと</p> <p>b.2 少なくとも年に 2 回</p> <p>根拠: FedRAMP v2</p> <p>-----</p>
<p>CP-2; 緊急事態対応計画; 緊急事態対応計画:</p> <p>組織:</p> <p>a. 情報システムのための緊急事態対応計画を策定</p> <ol style="list-style-type: none"> 1. 本質的なミッションとビジネス機能に関連した緊急時の要件を特定 2. 復旧の目標や復旧の優先順位の指標を提供 3. 緊急時の役割、責任を連絡先情報とともに特定 	<p>CP-2</p> <p>影響レベル 4-6:</p> <p>a. 少なくとも、ISSM と ISSO</p> <p>b. 緊急事態対応計画で特定されたすべてのステークホルダー</p> <p>f. 緊急事態対応計画で特定されたすべてのステークホルダー</p> <p>根拠: DoD RMF TAG</p> <p>-----</p>

<p>4. 情報システムの破壊、侵害や故障の事態でも維持すべきミッションやビジネス機能への取組み</p> <p>5. もともと計画され、実施されているセキュリティ保護手段を損なうことなく、最終的な完全な情報システム修復への取組み</p> <p>6. 次で審査・承認</p> <p>[設定：組織が定めた要員または役割];</p> <p>b. 緊急事態対応計画のコピーを次へ配布</p> <p>[設定：組織が定めた主要な緊急事態担当者（名前や役割によって識別される）や組織のエレメント];</p> <p>c. 事故処理活動と緊急事態の活動を調整</p> <p>d. 情報システムの緊急事態対応計画のレビュー</p> <p>[設定：組織が定めた頻度].</p> <p>e. 緊急事態対応計画を更新し、組織、情報システム、または運用環境や緊急事態対応計画の導入、実行、またはテスト中に発生した問題点の修正</p> <p>f. 緊急事態対応計画の変更</p> <p>[設定：組織が定めた主要な緊急事態担当者（名前や役割によって識別される）や組織のエレメント];</p> <p>そして</p> <p>g. 緊急事態対応計画の不正な開示や改ざんからの保護</p> <p>参照：連邦事業継続指令 1; NIST Special Publication 800-34.</p>	<p>すべての影響レベル：</p> <p>d. 少なくとも年に 1 回</p> <p>根拠：FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>要件：JAB 認可の場合、緊急時対応リストには指定された FedRAMP 要員を含む</p>
---	---

<p>CP-2 (3) ; 緊急事態対応計画; 緊急事態対応計画- 強化 :</p> <p>必須ミッション/ビジネス機能の再開</p> <p>組織は、緊要なミッションやビジネス機能の再開を計画</p> <p>[設定 : 組織が定めた期間]</p> <p>緊急事態対応計画の活性化</p> <p>参照 : なし</p>	<p>CP-2 (3)</p> <p>影響レベル 4-6 :</p> <p>1 時間 (可用性 高)</p> <p>12 時間 (可用性 中)</p> <p>緊急事態対応計画で定義されている。</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p>
<p>CP-3; 緊急事態対応計画; 緊急事態対応のトレーニング :</p> <p>組織は、割り当てられた役割と責任に沿って、情報システムのユーザに緊急事態対応のトレーニングを提供</p> <p>a. 次の期間内</p> <p>[設定 : 組織が定めた期間]</p> <p>緊急事態の役割または責任を想定</p> <p>b. 情報システムの変更が必要な場合—そして</p> <p>c. [設定 : 組織が定めた頻度]</p> <p>その後</p> <p>参照 : 連邦事業継続令 1 NIST Special Publications 800-16、800-50</p>	<p>CP-3</p> <p>すべての影響レベル :</p> <p>a. 10 日間</p> <p>c. 少なくとも年に 1 回</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>
<p>CP-4; 緊急事態対応計画; 緊急事態対応計画のテストと演習</p> <p>RENAMED : 緊急事態対応計画のテスト :</p> <p>組織 :</p> <p>a. 情報システムの緊急事態対応計画をテスト</p> <p>[設定 : 組織が定めた頻度]</p> <p>次を使って</p> <p>[設定 : 組織が定めたテスト]</p>	<p>CP-4</p> <p>影響レベル 4-6 :</p> <p>a. 少なくとも年に 1 回</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p>

<p>計画の有効性と計画を実行する組織の準備状況を決定</p> <p>b. 緊急時計画のテスト結果をレビュー そして</p> <p>c. 必要に応じて是正処置を開始</p> <p>参照：連邦事業継続令 1 FIPS Publication 199; NIST Special Publications 800-34, 800-84.</p>	<p>影響レベル 2：</p> <p>a. 中程度の影響度システムに対して少なくとも年 1 回；低の影響度システムでは少なくとも 3 年ごとに；中程度の影響度システムでは機能練習を実施；低の影響度システムでは、記述テストを含むクラスルーム/テーブルトップ演習を実施</p> <p>根拠：FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>a. 要件：サービスプロバイダは、NIST Special Publication 800-34（改正）に従って試験計画を作成。計画はテストの開始前に、認定官による承認を受ける。</p>
<p>CP-7；緊急事態対応計画；代替処理サイト：</p> <p>組織：</p> <p>a. 移転と再開を可能にするために必要な合意を含む代替処理サイトの設立</p> <p>〔設定：組織が定めた情報システムの運用〕</p> <p>緊要なミッション/ビジネス機能のために</p> <p>〔設定：リカバリ時間とリカバリポイントの目標と一貫性のある組織が定めた期間〕</p> <p>プライマリサイトの処理能力が利用できない場合</p> <p>b. 事業を移転・再開するために必要な設備と備品が代替処理サイトで利用可能であること、または移転/再開のために組織が定めた期間内に現場への納品を支援する契約があることを保証 ーそして</p> <p>c. 代替処理サイトがプライマリサイトと同等の情報セキュリティ保護を提供することを保証</p> <p>参照：NIST Special Publication 800-34.</p>	<p>CP-7</p> <p>影響レベル 4-6：</p> <p>a. 1 時間（可用性 高）緊急時対応計画で定義されている 12 時間（可用性 中）</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2：</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>CP-7a. 要件：サービスプロバイダは、復旧時間目標とビジネスインパクト分析と一致する期間を設定</p>

<p>CP-8; 緊急事態対応計画; 通信サービス :</p> <p>組織は、通信の再開を可能にするために必要な合意を含む代替通信サービスを確立</p> <p>設定 : 組織が定めた情報システムの運用]</p> <p>緊要なミッションやビジネス機能</p> <p>[割当 : 組織が定めた期間]</p> <p>プライマリまたは代替の処理やストレージサイトにおけるプライマリ通信が不能の場合</p> <p>参照 : NIST Special Publication 800-34; 国家通信令 3-10; Web : TSP.NCS.GOV</p>	<p>CP-8</p> <p>影響レベル 4-6 :</p> <p>1 時間 (可用性 高)</p> <p>12 時間 (可用性 中) 緊急事態対応計画で定義されている</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2 :</p> <p>FedRAMP 追加要件とガイダンス :</p> <p>CP-8. 要件 : サービスプロバイダは、ビジネス影響分析と一致する期間を設定</p>
<p>CP-9; 緊急事態対応計画; 情報システムバックアップ :</p> <p>組織 :</p> <p>a. 情報システムに含まれるユーザレベルの情報のバックアップを実行</p> <p>[設定 : リカバリタイムとリカバリポイントの目標が、組織の設定した頻度に合致]</p> <p>b. 情報システムに含まれるシステムレベルの情報のバックアップを実行</p> <p>[設定 : リカバリタイムとリカバリポイントの目標が、組織の設定した頻度に合致]</p> <p>c. セキュリティ関連の文書を含む情報システム文書のバックアップ</p> <p>[設定 : リカバリタイムとリカバリポイントの目標が、組織の設定した頻度に合致]</p> <p>そして</p>	<p>CP-9</p> <p>影響レベル 4-6 :</p> <p>c. 作成または受信されたとき、更新されたとき、または必要に応じて、緊急事態対応計画に従ってシステムのベースライン構成が変更されたとき</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル :</p> <p>a. 毎日増分; 毎週フル</p> <p>b. 毎日増分; 毎週フル</p>

<p>d. 保管場所におけるバックアップ情報の機密性、完全性、可用性を保護</p> <p>参照：NIST Special Publication 800-34.</p>	<p>影響レベル 2：</p> <p>c. 毎日増分;毎週フル</p> <p>根拠：FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>CP-9. 要件：サービスプロバイダは、情報システムバックアップコントロールを必要とするクラウド環境の要素を決定しなければならない。</p> <p>CP-9a. 要件：サービスプロバイダは、ユーザレベルの情報の少なくとも 3 つのバックアップコピーを保持（少なくとも 1 つはオンラインで利用可能）または同等の代替手段を提供すべき。</p> <p>CP-9b. 要件：サービスプロバイダは、システムレベルの情報の少なくとも 3 つのバックアップコピーを保持（少なくとも 1 つはオンラインで利用可能）または同等の代替手段を提供すべき。</p> <p>CP-9c. 要件：サービスプロバイダは、セキュリティ情報（少なくとも 1 つはオンラインで入手可能）を含む情報システム文書のバックアップコピーを少なくとも 3 つ保持するか、同等の代替手段を提供すべき。</p>
<p>CP-9（1）；緊急事態対応計画；情報システムバックアップ - 強化：</p> <p>信頼性/完全性のテスト</p> <p>組織はバックアップ情報をテスト</p> <p>[設定：組織が定めた頻度]</p>	<p>CP-9（1）</p> <p>影響レベル 4-6：</p> <p>緊急事態対応計画に従って少なくとも月に 1 回</p>

<p>メディアの信頼性と情報の完全性を検証</p> <p>参照：なし</p>	<p>根拠：DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2：</p> <p>少なくとも年に 1 回</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>CP-9（3）；緊急事態対応計画；情報システム バックアップ - 強化： 重大な情報のための別個のストレージ</p> <p>組織は、</p> <p>〔設定：組織が定めた重要な情報システムソフトウェアやその他のセキュリティ関連情報〕</p> <p>別の施設または運用システムと併置されていない耐火容器に保管</p> <p>参照：なし</p>	<p>CP-9（3）</p> <p>〔値は未設定。CSP により設定される〕</p>
<p>IA-1；識別と認証；識別と認証の方針と手順：</p> <p>組織：</p> <p>a. 開発、文書化、配布</p> <p>〔設定：組織が定めた要員または役割〕：</p> <p>1. 目的、範囲、役割、責任、管理コミットメント、組織間の調整、コンプライアンスに対応する識別認証ポリシー。そして</p> <p>2. 識別・認証方針や関連する識別・認証管理の実施を容易にする手順。および</p> <p>b. 現状のレビューと更新：</p> <p>1. 識別と認証ポリシー</p> <p>〔設定：組織が定めた頻度〕；</p>	<p>IA-1</p> <p>影響レベル 4-6：</p> <p>ISS0、ISSM、その他、該当の組織が適切とみなす；</p> <p>b. 1 毎年</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2：</p> <p>b. 1 少なくとも 3 年ごと</p>

<p>2. 識別と認証手順</p> <p>[設定：組織が定めた頻度].</p> <p>参照：FIPS Publication 201; NIST Special Publications 800-12, 800-63, 800-73, 800-76, 800-78, 800-100</p>	<p>すべての影響レベル：</p> <p>b.2 少なくとも毎年</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>IA-2 (11)；識別と認証；識別と認証（組織ユーザ） - 強化：</p> <p>リモートアクセス - デバイスの分離</p> <p>情報システムは、特権および非特権アカウントへのリモートアクセスのために多要素の認証を実装し、システムのアクセスとは別のデバイスによって要素の1つが提供され、デバイスは次を満たす</p> <p>[設定：組織が定めた強度のメカニズム要件]</p> <p>参照：なし</p>	<p>IA-2 (11)</p> <p>影響レベル 4-6：</p> <p>DoD PKI や認定担当官の承認, FIPS 140-2, NIAP 認定、または NSA の承認を受けた技術</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>
<p>IA-3；識別と認証；デバイスの識別と認証：</p> <p>情報システムは、一意に識別し、認証する</p> <p>[設定：組織が定めた特定・デバイスタイプのリスト]次を確立する前に</p> <p>[選択（1つまたは複数）：</p> <ul style="list-style-type: none"> - ローカル； - リモート； - ネットワーク <p>]</p> <p>接続</p> <p>参照：なし</p>	<p>IA-3</p> <p>影響レベル 4-6：</p> <p>ワークステーション、プリンタ、サーバー（データセンター外）、VoIP 電話機、VTC CODEC など、すべてのモバイルデバイスとネットワーク接続されたエンドポイントデバイスを含む。</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>

<p>IA-4; 識別と認証; 識別子管理 :</p> <p>組織は、次の方法で情報システム識別子を管理</p> <p>a. 次の承認を受ける</p> <p style="color: red;">[設定 : 組織が定めた要員または役割]</p> <p>個人、グループ、役割、またはデバイス識別子の割当</p> <p>b. 個人、グループ、役割、またはデバイスを識別する識別子の選択</p> <p>c. 意図した個人、グループ、役割、またはデバイスに識別子の割当</p> <p>d. 再利用の防止</p> <p style="color: red;">[設定 : 組織が定めた期間]; そして</p> <p>e. 識別子の無効化</p> <p style="color: red;">[設定 : 組織が定めた非活動期間]</p> <p>参照 : FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78.</p>	<p>IA-4</p> <p>影響レベル 4-6 :</p> <p>a. ISSM または ISSO</p> <p>e. 35 日</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル :</p> <p>d. 少なくとも 2 年間</p> <p>影響レベル 2 :</p> <p>e. ユーザ識別子では 90 日間 (追加の要件とガイダンスを参照)</p> <p>根拠 : FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス :</p> <p>IA-4e. 要件 : サービスプロバイダは、デバイス識別子の非アクティブ期間を定義</p>
<p>IA-4 (4) ; 識別と認証; 識別子管理 - 強化 :</p> <p>ユーザステータスの識別</p> <p>組織は、各個人を一意に識別することにより、個人の識別子を管理</p> <p style="color: red;">[設定 : 組織が定めた個人のステータスを識別する特徴]</p> <p>参照 : なし</p>	<p>IA-4 (4)</p> <p>影響レベル 4-6 :</p> <p>請負業者または公務員及び国籍による。ユーザ ID は、DoD ユーザの電子メールアドレス (john.smith.ctr@army.mil や john.smith.uk@army.mil) と同じ形式に従う。</p> <p>- DoD ユーザの電子メール表示名 (例えば、John Smith、Contractor <john.smith.ctr@army.mil>または英国の</p>

	<p>John Smith、 <john.smith.uk@army.mil>) ; そして 自動署名ブロック (例えば、John Smith、 Contractor, J-6K, Joint Staff または John Doe, Australia, LNO, Combatant Command)。 外国人でもある請負業者は、例えば、 john.smith.ctr.uk@army.mil</p> <p>根拠 : DoD RMF TAG -----</p> <p>影響レベル 2 : 請負業者。 外国人</p> <p>根拠 : FedRAMP v2 -----</p>
<p>IA-5;識別と認証; 認証管理 :</p> <p>組織は、次の方法で情報システム認証を管理</p> <p>a. 最初に認証を配布する際の、認証を受領する個人、グループ、ロール、またはデバイスの身元を確認</p> <p>b. 組織で定義した認証の初期値内容の確立</p> <p>c. 認証が意図された用途に十分な強度の機構を持つことの保証</p> <p>d. 認証の初期配布、紛失/侵害、破損や失効時の管理手順の確立</p> <p>e. 情報システムのインストール前に、認証の既定値の変更</p> <p>f. 認証の最小・最大の有効期間制限と再使用条件の確立</p> <p>g. 認証の変更/更新</p>	<p>IA-5</p> <p>影響レベル 4-6 :</p> <p>g. CAC - 3 年ごと、または契約期間から 1 年間</p> <p>パスワード : 60 日</p> <p>バイオメトリクス : 3 年ごとに再登録</p> <p>根拠 : DoD RMF TAG -----</p> <p>影響レベル 2 :</p> <p>g. パスワードに 60 日</p> <p>根拠 : FedRAMP v2 -----</p>

<p>[設定：認証タイプに応じて組織が定めた期間]；</p> <p>h. 認証の内容を不正な開示や改ざんから保護—そして</p> <p>i. 個人が認証を保護するための特定のセキュリティ保護手段を講じ、デバイスを実装することの要求—そして</p> <p>j. アカウントのメンバーシップが変更されたときの、グループ/ロールアカウントの認証変更</p> <p>参照：OMB 覚書 04-04, 11-11； FIPS Publication 201； NIST Special Publications 800-73, 800-63, 800-76, 800-78； FICAM のロードマップと実装ガイダンス； Web：idmanagement.gov</p>	
<p>IA-5 (1) ；識別と認証；認証管理 – 強化：パスワードベースの認証</p> <p>パスワードベースの認証のための情報システム：</p> <p>a. パスワードの最小限の複雑さの強制</p> <p>[設定：組織が定めた大文字／小文字の区別、文字数、大文字、小文字、数字、記号の混在と各種類の最小要件]；</p> <p>b. 新しいパスワードを作成するときに、少なくとも次の変更文字数を適用</p> <p>[設定：組織が定めた数]；</p> <p>c. 暗号化された形式のパスワードのみを格納し、送信</p> <p>d. パスワードの最小および最大の有効期限を強制</p> <p>[設定：組織が定めた有効期間の最大]；</p> <p>e. パスワードの再利用禁止</p> <p>[設定：組織が定めた数]</p>	<p>IA-5 (1)</p> <p>影響レベル 4-6：</p> <p>デバイスで利用可能な：</p> <p>a. 最低 15 文字、次の文字セットからそれぞれ各 1 を含む</p> <ul style="list-style-type: none">– 大文字– 小文字– 数値– 記号（例：~!@#%&* () _ + = - ' [] /?><)] ; , <p>根拠：DoD RMF TAG</p> <p>-----</p>

<p>世代—そして</p> <p>f. 一時パスワードを使ってシステムへログインし、即時に恒久パスワードを即座に変更することの許可</p> <p>参照：なし</p>	<p>影響レベル 2：</p> <p>a. 大文字と小文字を区別し、最小 12 文字、大文字、小文字、数字、および記号の各 1 つ以上</p> <p>すべての影響レベル：</p> <p>b. 少なくとも一つ</p> <p>d. 最小 1 日、最大 60 日</p> <p>e. 24</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>IA-5 (3)；識別と認証；認証管理 - 強化：人または信頼できる第三者登録</p> <p>組織には、受領のための登録プロセスとして以下が必要</p> <p> [設定：組織が定めたタイプ・特定の認証]</p> <p>以下で実施</p> <p> [選択：</p> <p> - 自分</p> <p> - 信頼できる第三者による</p> <p>]</p> <p>前に</p> <p> [設定：組織が定める登録機関]</p> <p>次の認可を得て</p> <p> [設定：組織が定めた要員または役職].</p> <p>参照：なし</p>	<p>IA-5 (3)</p> <p>影響レベル 4-6：</p> <p>DoD PKI CP は、DoD PKI Registration Authority (RA) の役割と責任を定義している。NSS PKI CP は、NSS PKI RA の役割と責任を定義している。</p> <p>DoD PKI RA-LRA CPS は、DoD PKI RA のノミネーション・プロセスを定義している。NSS PKI DoD RPS は、DoD のための NSS PKI RA のノミネーション・プロセスを定義している。</p> <p>DoD PKI CP は、DoD PKI ユーザと、ユーザに対するクレデンシャルの発行に関する認証要件を定義している。NSS PKI CP は、NSS PKI サブスクライバと、サブスクライバへのクレデンシャルの発行に関する認証要件を定義している。</p>

	<p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2 :</p> <p>すべてのハードウェア/バイオメトリック (多要素認証)</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>
<p>IA-5 (4) ; 識別と認証; 認証管理 - 強化 : パスワード強度決定の自動サポート</p> <p>組織は自動化されたツールを使用して、パスワード認証が十分に強力であるかどうかを判断</p> <p>[設定 : 組織が定めた要件].</p> <p>参照 : なし</p>	<p>IA-5 (4)</p> <p>影響レベル 4-6 :</p> <p>IA-5 (1) Part A で決められた複雑</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル :</p> <p>FedRAMP 追加要件とガイダンス :</p> <p>IA-4e 追加の FedRAMP 要件とガイダンスガイダンス : 作成時にパスワード認証の強度を強制する自動化メカニズムが使用されていない場合、作成されたパスワード認証の強度を自動化するメカニズムを使用する必要がある。</p>
<p>IA-5 (11) ; 識別と認証; 認証管理 - 強化 : ハードウェアトークンベースの認証</p> <p>情報システムは、次を満たすハードウェアトークンベースの認証を採用</p> <p>[設定 : 組織が定めたトークンの品質要件]</p> <p>参照 : なし</p>	<p>IA-5 (11)</p> <p>影響レベル 4-6 :</p> <p>DoDI 8520.03</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p>

<p>IA-5 (13) ; 識別と認証; 認証管理 - 強化 : キャッシュされた認証の有効期限</p> <p>情報システムは、次の規定以降のキャッシュ された認証の使用を禁止</p> <p>[設定 : 組織が定めた時間]</p> <p>参照 : なし</p>	<p>IA-5 (13)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>IA-8 (3) ; 識別と認証; 識別と認証 (非組織 ユーザ) - 強化 : FICAM 認定製品の使用</p> <p>組織は次について、FICAM が承認した情報シス テムコンポーネントのみを採用</p> <p>[設定 : 組織が定めた情報システム]</p> <p>サードパーティの資格情報の受入れ</p> <p>参照 : なし</p>	<p>IA-8 (3)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>IR-1; インシデントレスポンス ; インシデン ト・レスポンスの方針と手順 :</p> <p>組織 :</p> <p>a. 開発、文書化、配布</p> <p>[設定 : 組織が定めた要員または役割] :</p> <ol style="list-style-type: none"> 1. 目的、範囲、役割、責任、管理、コミッ トメント、組織間の調整、コンプライア ンスに言及したインシデントレスポンス の方針 2. インシデントレスポンスの方針や関連す るインシデントレスポンスのコントロー ルの実施を容易にする手順 <p>b. 現状のレビューと更新 :</p> <ol style="list-style-type: none"> 1. インシデントレスポンスの方針 <p>[設定 : 組織が定めた頻度];</p>	<p>IR-1</p> <p>影響レベル 4-6 :</p> <p>a. インシデント・レスポンスプロセスに おいてステークホルダーとして特定された すべての要員、ISSM および ISSO</p> <p>根拠 : DoD RMF TAG -----</p> <p>すべての影響レベル :</p> <p>b. 1 少なくとも 3 年ごと</p> <p>b. 2 少なくとも年に 1 回</p> <p>根拠 : FedRAMP v2 -----</p>

<p>2. インシデントレスポンスの手順 [設定：組織が定めた頻度].</p> <p>参照：NIST Special Publications 800-12、 800-61, 800-83, 800-100.</p>	
<p>IR-2; インシデントレスポンス ; インシデントレスポンス訓練 :</p> <p>組織は、割り当てられた役割と責任に対応したインシデント・レスポンス訓練を情報システムのユーザに提供</p> <p>a. 次の期間内 [割当：組織が定めた期間] インシデントレスポンスの役割と責任を引受け</p> <p>b. 情報システムの変更が必要な場合 ; そして</p> <p>c. [設定：組織が定めた頻度]</p> <p>参照：NIST Special Publications 800-16, 800-50.</p>	<p>IR-2</p> <p>影響レベル 4-6 :</p> <p>a. 30 営業日</p> <p>根拠 : DoD の RMF TAG -----</p> <p>すべての影響レベル :</p> <p>c. 少なくとも年に 1 回</p> <p>根拠 : FedRAMP v2 -----</p>
<p>IR-3; インシデントレスポンス ; インシデントレスポンスのテストと演習 RENAMED : インシデント・レスポンス・テスト :</p> <p>組織は、情報システムのインシデントレスポンス能力をテスト</p> <p>[設定：組織が定めた頻度] を使用して</p> <p>[設定：組織が定めたテスト] インシデントレスポンスの有効性を判断し、 結果を文書化</p>	<p>IR-3</p> <p>影響レベル 4-6 :</p> <p>高可用性では、少なくとも 6 ヶ月に 1 回、 低/中では少なくとも 1 年に 1 回。</p> <p>インシデントレスポンス計画で定義されているテスト</p> <p>根拠 : DoD RMF TAG -----</p>

<p>参照：NIST Special Publications 800-84, 800-115.</p>	<p>影響レベル 2： 少なくとも年に 1 回</p> <p>根拠：FedRAMP v2 -----</p> <p>FedRAMP 追加要件とガイダンス： IR-3. 要件：サービスプロバイダは、NIST Special Publication 800-61（改訂版）に従って試験や演習を定義。 要件：JAB 認可の場合、サービスプロバイダは認定担当官（AO）へ毎年テスト計画を提供 要件：テストの計画は、試験開始前に認定担当官に承認される。</p>
<p>IR-4(3)；インシデントレスポンス；インシデント処理－強化： 運用コミュニティ 組織は、次を明確化 [設定：組織が定めたインシデントの規模] [設定：組織が定めたインシデントの規模に応じて実行する対処] 確実に組織のミッションとビジネス機能を継続</p>	<p>IR-4（3）</p> <p>影響レベル 4-6： CJCSM 6510.01B で定義されているインシデントのクラス付録 A-エンクロージャーB CJCSM 6510.01B で定義されているアクション 根拠：DoD RMF TAG -----</p>
<p>IR-4（7）；インシデントレスポンス；インシデント処理－強化： インサイダーの脅威－組織内の調整 組織は、内部の脅威に対するインシデントレスポンス能力を調整 [設定：組織が定めた組織のコンポーネントまたは要素]. 参照：なし</p>	<p>IR-4（7） [値は未設定。CSP により設定される]</p>

<p>IR-4 (8) ; インシデントレスポンス ; インシデント処理 - 強化 :</p> <p>外部組織との相関</p> <p>組織は次と調整</p> <p>〔設定 : 組織が定めた外部組織〕</p> <p>調整して共有</p> <p>〔設定 : 組織が定めたインシデント情報〕</p> <p>インシデントの意識高揚とより効果的なインシデント処理に関する組織を超えた視点の実現</p> <p>参照 : なし</p>	<p>IR-4 (8)</p> <p>影響レベル 4-6 :</p> <p>適切な CIRT/CERT (US-CERT、DoD CERT、IC CERT など)、ミッションオーナーの MCD、や司法機関</p> <p>セクション 6.4 - サイバーインシデントレポートと対処に定義されているインシデント情報</p> <p>根拠 : DoD RMF TAG (商用 CSP 向けの調整を含む)</p> <p>-----</p>
<p>IR-6; インシデントレスポンス ; インシデントレポート :</p> <p>組織 :</p> <p>a. 職員には、疑わしいセキュリティ・インシデントを組織内のインシデント・レスポンス部門へ、次の時間内に報告</p> <p>〔設定 : 組織が定めた期間〕;</p> <p>そして</p> <p>b. セキュリティインシデント情報をレポート</p> <p>〔設定 : 組織が定めた権限〕.</p> <p>参照 : NIST Special Publication 800-61 :</p> <p>Web : WWW.US-CERT.GOV</p>	<p>IR-6</p> <p>影響レベル 4-6 :</p> <p>a. データ所有者がより限定的なガイダンスを提供しない限り、CJCSM 6510.01B (表 C-A-1) で指定された時間内</p> <p>b. 適切な CIRT/CERT (US-CERT、DoD CERT、IC CERT など)、ミッションオーナーの MCD、および司法機関</p> <p>根拠 : DoD RMF TAG (商用 CSP の調整を含む)</p> <p>-----</p> <p>影響レベル 2 :</p> <p>a. NIST Special Publication 800-61 (改正) に規定されている US-CERT インシデント報告のタイムライン</p>

	<p>根拠 : FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス :</p> <p>要件 : FedRAMP Incident Communications Procedure に従ってセキュリティインシデント情報を報告</p>
<p>IR-6 (2) ; インシデントレスポンス ; インシデントレポート - 強化 :</p> <p>インシデントに関連する脆弱性</p> <p>組織は、報告されたセキュリティインシデントに関連する情報システムの脆弱性を次へ報告</p> <p>[設定 : 組織が定めた要員または役割].</p> <p>参照 : なし</p>	<p>IR-6 (2)</p> <p>すべての影響レベル :</p> <p>PA と顧客の ATO を発行した A0、顧客の MCD、CIRT/CERT (US-CERT, DoD CERT, IC CERT など)</p> <p>根拠 : コミュニティの情報共有とコミュニティ全体の新しい脆弱性の緩和のための CC SRG ベストプラクティス</p>
<p>IR-8; インシデントレスポンス ; インシデント・レスポンス計画 :</p> <p>組織 :</p> <p>a. インシデントレスポンス計画を策定</p> <ol style="list-style-type: none">1. インシデントレスポンス機能を実装するためのロードマップを組織へ提供2. インシデントレスポンス機能の構造と組織を記述3. インシデントレスポンス機能が組織全体にどのように適合するかについて、高レベルのアプローチを提供4. ミッション、規模、構成と機能に関連した組織の固有の要件に合致5. 報告可能なインシデントを定義6. 組織内のインシデントレスポンス能力を測定するための指標を提供	<p>IR-8</p> <p>影響レベル 4-6 :</p> <p>a. 少なくとも、ISSM と ISSO</p> <p>b. インシデントレスポンス計画で特定されたすべてのステークホルダー</p> <p>e. 変更後 30 日以内に、インシデント・レスポンス計画で特定されたすべてのステークホルダー</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル :</p> <p>c. 少なくとも年に 1 回</p>

<p>7. インシデントレスポンス機能を効果的に維持・成熟させるために必要なリソースと管理サポートを定義 そして</p> <p>8. 次によるレビューと承認 [設定：組織が定めた要員または役割]；</p> <p>b. インシデントレスポンス計画のコピーを次へ配布 [設定：組織が定めたインシデントレスポンスの要員（名前・役割別）と組織部門].</p> <p>c. インシデントレスポンス計画のレビュー [設定：組織が定めた頻度].</p> <p>d. インシデント・レスポンス計画の更新、計画、実装、またはテストの計画中に発生したシステム/組織の変更または問題に対処</p> <p>e. インシデント・レスポンス計画の変更を次へ伝達 [設定：組織が定めたインシデントレスポンス要員名前・役割で識別される）と組織部門]；</p> <p>そして</p> <p>f. インシデント・レスポンス計画の不正な開示と変更からの保護</p> <p>参照：NIST Special Publication 800-61</p>	<p>根拠：FedRAMP v2 -----</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>IR-8 (b) 追加の FedRAMP 要件およびガイダンス：サービス提供者は、（名前・役割によって識別される）インシデントレスポンス担当者のリストと組織部門を定義する。インシデント・レスポンスリストには、指定された FedRAMP 担当者が含まれる。</p> <p>IR-8 (e) 追加の FedRAMP 要件とガイダンス：サービス提供者は、インシデントレスポンス担当者（名前・役割によって識別される）と組織部門のリストを定義する。インシデント・レスポンスリストには、指定された FedRAMP 担当者が含まれる。</p>
<p>IR-9； インシデントレスポンス； 情報流出対処：</p> <p>組織は情報の流出に以下の方法で対処</p> <p>a. 情報システムの侵害に関わる特定の情報の明確化</p> <p>b. 情報の流出を警告 [設定：組織が定めた要員または役割]</p> <p>流出とは無関係な通信手段を使用</p>	<p>IR-9</p> <p>影響レベル 4-6：</p> <p>b. 最低限、OCA、情報所有者/発信者、ISSM、アクティビティセキュリティマネージャー、責任を負うコンピュータインシデント・レスポンスセンター</p> <p>根拠：DoD RMF TAG -----</p>

<p>c. 侵害された情報システムやシステムコンポーネントの分離</p> <p>d. 侵害された情報システムやコンポーネントからの情報の駆除</p> <p>e. 2 次的に侵害された可能性がある他の情報システムまたはシステムコンポーネントの特定。そして</p> <p>f. その他の実行</p> <p>[設定：組織が定める行動].</p> <p>参照：なし</p>	<p>f. 被害やアクセスの量を局限するため、迅速な対処。対処の日時を含む CS/IA インシデント・レスポンスに関するすべてのアクションのログを保持。その役割に応じて、チケットなどの記録を作成し管理。</p> <p>根拠：DoD ベストプラクティス</p> <p>-----</p>
<p>IR-9 (1) ; インシデントレスポンス ; 情報流出対処 - 強化 :</p> <p>責任者</p> <p>組織は、</p> <p>[設定：組織が定めた要員または役割]</p> <p>情報の流出に対処する責任がある。</p> <p>参照：なし</p>	<p>IR-9 (1)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>IR-9 (2) ; インシデントレスポンス ; 情報流出対処 - 強化 :</p> <p>トレーニング</p> <p>組織は情報流出対処トレーニングを提供する。</p> <p>[設定：組織が定めた頻度].</p> <p>参照：なし..</p>	<p>IR-9 (2)</p> <p>影響レベル 4-6 :</p> <p>毎年</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>
<p>IR-9 (3) ; インシデントレスポンス ; 情報流出対処 - 強化 :</p> <p>流出後の運用</p> <p>組織は、次を実行</p> <p>[設定：組織が定めた手続き]</p>	<p>IR-9 (3)</p> <p>[値は未設定。 CSP により設定される]</p>

<p>侵害されたシステムが是正措置を受けている間に、情報の流出によって影響を受けた組織の要員が引き続き割り当てられたタスクを実行できるようにする。</p> <p>参照：なし</p>	
<p>IR-9 (4) ; インシデントレスポンス ; 情報流出対処 - 強化 :</p> <p>権限のない人への発覚</p> <p>組織は、割り当てられたアクセス許可範囲外で、情報に晒された人員に対し、次を実行</p> <p>[設定：組織が定めたセキュリティ保護手段]</p> <p>参照：なし</p>	<p>IR-9 (4)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>MA-1; メンテナンス; システムメンテナンス方針と手順:</p> <p>組織:</p> <p>a. 開発、文書化、配布</p> <p>[設定：組織が定めた要員または役割]:</p> <ol style="list-style-type: none"> 1. 目的、範囲、役割、責任、管理を扱うシステム保守ポリシー、コミットメント、組織間の調整、コンプライアンスに言及したシステムメンテナンスの方針 2. システムメンテナンス方針や関連するメンテナンスコントロールの実施を円滑にするための手順 <p>そして</p> <p>b. 現状のレビューと更新:</p> <ol style="list-style-type: none"> 1. システムメンテナンスの方針 <p>[設定：組織が定めた頻度].</p> <p>そして</p> <ol style="list-style-type: none"> 2. システムメンテナンス手順 	<p>MA-1</p> <p>影響レベル 4-6 :</p> <p>a. メンテナンスポリシーで特定されたすべてのステークホルダー</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル:</p> <p>b. 1 少なくとも 3 年ごと</p> <p>b. 2 少なくとも年 1 回</p> <p>根拠：FedRAMP v2</p> <p>-----</p>

<p>[設定：組織が定めた頻度].</p> <p>参照：NIST Special Publications 800-12, 800-100.</p>	
<p>MA-2;メンテナンス;コントロールされたメン テナンス：</p> <p>組織：</p> <p>a. 製造元、ベンダーの仕様や組織の要件に従 って、情報システムコンポーネントのメンテ ナンスや修理の記録のスケジュール、実行、 文書化とレビュー</p> <p>b. ローカル／リモートで実施、現場で修理／ 別の場所へ移送などを問わず、すべてのメン テナンス作業の監視と承認</p> <p>c. 次について、明示的な承認が必要</p> <p>[設定：組織が定めた要員または役割]</p> <p>オフサイトでの保守や修理のために情報シス テムまたはシステムコンポーネントを組織の 施設から外す行為</p> <p>d. オフサイトのメンテナンスや修理のために 組織の施設から取り外す前に、関連するメデ ィアからすべての情報を削除するように装置 のサニタイズ</p> <p>e. 影響を受ける可能性のあるすべてのセキュ リティ管理策をチェックし、コントロールが メンテナンスまたは修理やメンテナンス後も 適切に機能していることを確認</p> <p>f. 組織のメンテナンス記録に次を含む</p> <p>[設定：組織が定めた保守関連情報]</p> <p>参照：なし</p>	<p>MA-2</p> <p>[値は未設定。 CSP により設定される]</p>

<p>MA-3 (3) ; メンテナンス; メンテナンス・ツール - 機能強化 :</p> <p>許可のない取り外しの防止</p> <p>組織は、組織の情報を含む保守機器を許可なしに取り外しを次により防止</p> <p>a. 機器に組織の情報が含まれていないことを確認</p> <p>b. 機器のサニタイズまたは破壊;</p> <p>c. 施設内へ機器を保持。または</p> <p>d. 次による免除</p> <p>[設定: 組織が定めた要員または役割]</p> <p>施設からの機器の取り外しの明示的な許可</p> <p>参照: なし</p>	<p>MA-3 (3)</p> <p>すべての影響レベル:</p> <p>d. 情報所有者が施設からの機器の取り外しを明示的に許可</p> <p>根拠: FedRAMP v2</p> <p>-----</p>
<p>MA-6; メンテナンス; タイムリーメンテナンス:</p> <p>組織は、メンテナンスサポートやスペアパーツを保持</p> <p>[設定: 組織が定めた情報システムコンポーネント]</p> <p>次の期間内</p> <p>[割当: 組織が定めた期間]</p> <p>故障時</p> <p>参照: なし</p>	<p>MA-6</p> <p>影響レベル 4-6:</p> <p>CSO SLA に従うか、最低でも次による。</p> <p>24 時間以内 (低・中可用性)、または障害発生直後 (高可用性)</p> <p>根拠: DoD RMF TAG</p> <p>-----</p>
<p>MP-1; 媒体保護; 媒体保護方針と手順:</p> <p>組織:</p> <p>a. 開発、文書化、配布</p> <p>[設定: 組織が定めた要員または役割]:</p> <p>1. 媒体の保護方針、目的、範囲、役割、責任、管理コミットメント、組織エンティ</p>	<p>MP-1</p> <p>影響レベル 4-6:</p> <p>a. すべてのユーザ</p> <p>根拠: DoD RMF TAG</p> <p>-----</p>

<p>ティ間の調整、コンプライアンス、そして</p> <p>2. 媒体の保護方針と媒体の保護コントロールに関連した手続きの策定</p> <p>そして</p> <p>b. 現状のレビューと更新：</p> <p>1. 媒体保護方針</p> <p>[設定：組織が定めた頻度]；そして</p> <p>2. メディア保護手順</p> <p>[設定：組織が定めた頻度].</p> <p>参照：NIST Special Publications 800-12, 800-100.</p>	<p>すべての影響レベル：</p> <p>b.1 少なくとも3年ごと</p> <p>b.2 少なくとも年に1回</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>MP-2；媒体保護；媒体のアクセス：</p> <p>組織は、次のアクセスを制限</p> <p>[設定：組織が定めたデジタル・非デジタルメディア]</p> <p>次に対し</p> <p>[設定：組織が定めた要員または役割].</p> <p>参照：FIPS Publication 199；NIST Special Publication 800-111.</p>	<p>MP-2</p> <p>影響レベル 4-6：</p> <p>一般公開用として許可されていない情報を含むすべての種類のデジタルメディア・非デジタルメディア</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>
<p>MP-3；媒体保護；メディアマーキング：</p> <p>組織：</p> <p>a. 情報の配布制限、取り扱いの注意点や該当するセキュリティマーキング（存在する場合）を示す情報システム・媒体にマークする。そして</p> <p>b. 次の条件でマーキングを免除</p> <p>[設定：組織が定めたタイプのシステム・媒体情報]</p> <p>メディア次に所在する限り</p> <p>[設定：組織が定める管理区域].</p>	<p>MP-3</p> <p>影響レベル 4-6：</p> <p>b. DoDI 5200.01 および DoDM 5200.01 第1-4巻で別途免除されない限り</p> <p>b. DoD 5200.01 および DoDM 5200.01 第1-4巻で免除されない限り、すべての領域</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>

<p>参照 : FIPS Publication 199</p>	<p>影響レベル 2 :</p> <p>b. リムーバブルメディアタイプでない場合</p> <p>根拠 : FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス :</p> <p>MP-3b. ガイダンス : 第 2 パラメータは適用不可</p>
<p>MP-4; 媒体保護; 媒体の保管 :</p> <p>組織 :</p> <p>a. 物理的なコントロールと安全な保管</p> <p> [設定 : 組織が定めたデジタル・非デジタルメディア]</p> <p>範囲内</p> <p> [設定 : 組織が定めた管理区域];</p> <p>そして</p> <p>b. 承認された機器、技術、および手順を使用して媒体を破壊またはサニタイズされるまで、情報システム・媒体を保護</p> <p>参照 : FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-11</p>	<p>MP-4</p> <p>影響レベル 4-6 :</p> <p>a. 1 センシティブやコントロールまたは格付けされた情報を含むすべてのデジタル・非デジタルメディア。</p> <p>a. 2 メディアに含まれる情報の機微性、格付けのレベルに従って、処理やデータの保管が許可された領域。</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2 :</p> <p>a. 機微な情報を含むあらゆるタイプのデジタルメディアと非デジタルメディア</p> <p>FedRAMP の指定 : FedRAMP の追加要件とガイダンスを参照</p> <p>根拠 : FedRAMP v2</p>

	<p>-----</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>MP-4a 追加の FedRAMP 要件とガイダンス：</p> <p>要件：サービスプロバイダは、情報および情報システムが存在する施設内の管理区域を定義。</p>
<p>MP-5； 媒体保護；媒体の輸送：</p> <p>組織：</p> <p>a. 保護とコントロール</p> <p> [設定：組織が定めた種類のシステム・媒体情報]</p> <p>管理区域外での輸送中に</p> <p> [設定：組織が定めたセキュリティ保護手段]；</p> <p>b. 管理区域外の輸送中に情報システム媒体の管理責任を維持</p> <p>c. 情報システム媒体の輸送に関連する活動を文書化</p> <p>d. 情報システム媒体の輸送に関連する活動を、許可された要員に制限</p> <p>参照：FIPS Publication 199； NIST Special Publication 800-60</p>	<p>MP-5</p> <p>影響レベル 4-6：</p> <p>a. 機微、コントロールや格付された情報を含むすべてのデジタルメディアと非デジタルメディア。</p> <p>a. DoDI 5200.1R およびその他の組織で定義されたセキュリティ保護手段を提供。</p> <p>根拠：DoD RMF TAG と FedRAMP v2</p> <p>-----</p> <p>影響レベル 2：</p> <p>a. 機微な情報を含むすべてのメディア</p> <p>安全に管理された環境を離れる前に：デジタルメディアの場合は、FIPS 140-2 検証済み暗号化モジュールを使用した暗号化；非デジタルメディアではロックされたコンテナに格納</p> <p>根拠：FedRAMP v2</p> <p>-----</p>

<p>MP-6; 媒体保護; 媒体サニタイズ:</p> <p>組織:</p> <p>a. サニタイズ</p> <p>[設定: 組織が定めた情報システムの媒体]</p> <p>処分する前に、組織の管理から解放するか、または</p> <p>[設定: 組織が定めたサニタイズ技術と手順]</p> <p>適用される連邦/組織の基準や方針に従って — そして</p> <p>b. セキュリティカテゴリまたは情報の分類に見合った強度と完全性を備えたサニタイズ機構を採用</p> <p>参照: FIPS Publication 199; NIST Special Publications 800-60、800-88; Web: www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml</p>	<p>MP-6</p> <p>影響レベル 4-6:</p> <p>a. すべてのメディア</p> <p>a. NIST SP 800-88 およびセクション 5.9: ストレージメディアとハードウェアの再利用と廃棄を参照</p> <p>根拠: DoD RMF TAG</p> <p>-----</p>
<p>MP-6 (2); 媒体保護; メディアのサニタイズ - 強化:</p> <p>機器試験</p> <p>組織はサニタイズ設備と手順をテストする</p> <p>[設定: 組織が定めた頻度]</p> <p>意図したサニタイズが達成されていることを確認</p> <p>参照: なし</p>	<p>MP-6 (2)</p> <p>影響レベル 4-6:</p> <p>180 日ごとに</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2:</p> <p>少なくとも毎年</p> <p>根拠: FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス:</p>

	<p>ガイダンス：機器および手順の有効性をテストまたは検証する。</p>
<p>MP-7; 媒体保護; 媒体の使用:</p> <p>組織は[選択: 制限; 使用の禁止] 次の利用を</p> <p>[設定: 組織が定めた情報の種類システム・媒体]</p> <p>次について</p> <p>[設定: 組織が定めた情報システムまたはシステム構成要素]</p> <p>次を利用して</p> <p>[設定: 組織が定めたセキュリティ保護手段].</p> <p>参照: FIPS Publication 199; NIST Special Publication 800-111</p>	<p>MP-7</p> <p>[値は未設定。 CSP により設定される]</p>
<p>PE-1; 物理的および環境的防護; 物理的および環境保護の方針と手続き:</p> <p>組織:</p> <p>a. 開発、文書化、配布</p> <p>[設定: 組織が定めた要員または役割]:</p> <p>1. 目的、範囲、役割、責任、責任、経営者のコミットメント、組織間の調整、コンプライアンスを述べた物理的・環境的防護の方針</p> <p>そして</p> <p>2. 物理的・環境的防護の方針や関連する物理的・環境的防護コントロールの実施を促進するための手続</p> <p>そして</p>	<p>PE-1</p> <p>影響レベル 4-6:</p> <p>a. すべての人員</p> <p>毎年 b. 1</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2:</p> <p>b. 1 少なくとも 3 年ごと</p> <p>すべての影響レベル:</p>

<p>b. 現状のレビューと更新：</p> <p>1. 物理的・環境的防護の方針 [設定：組織が定めた頻度]。 そして</p> <p>2. 物理的・環境的な防護手順 [設定：組織が定めた頻度]。</p> <p>参照：NIST Special Publications 800-12, 800-100</p>	<p>少なくとも年に2回</p> <p>根拠：FedRAMP v2 -----</p>
<p>PE-2；物理的・環境的防護；物理アクセス権 限：</p> <p>組織：</p> <p>a. 情報システムが所在する施設へのアクセス が許可された個人リストの作成、承認、維持</p> <p>b. 施設へのアクセスの認可資格の発行</p> <p>c. 個人による認可された施設へのアクセスを 詳述するアクセスリストのレビュー [設定：組織が定めた頻度]</p> <p>そして</p> <p>d. アクセスが不要になった際の施設アクセス リストからの削除</p> <p>参照：なし</p>	<p>PE-2</p> <p>影響レベル 4-6： c. 90 日ごと</p> <p>根拠：DoD RMF TAG -----</p> <p>影響レベル 2： c. 少なくとも年に1回</p> <p>根拠：FedRAMP v2 -----</p>
<p>PE-3；物理的および環境的防護；物理的アクセ スコントロール：</p> <p>組織：</p> <p>a. 次の物理的なアクセス許可を強制 [設定：組織が定めた情報システムが常駐す る施設の出入口]</p> <p>以下の手段で；</p> <p>1. 施設へのアクセスを許す前に、個々のア クセス許可を確認；そして</p>	<p>PE-3</p> <p>影響レベル 4-6：</p> <p>f. 少なくとも鍵、またはアクセスに使用 されるその他の物理的トークン</p> <p>g. セキュリティ関連のイベントで必要と される都度、少なくとも毎年</p> <p>根拠：DoD RMF TAG と FedRAMP v2</p>

<p>2. 以下による施設への出入り口のコントロール</p> <p>[選択 (1 つまたは複数) :</p> <ul style="list-style-type: none">- [設定 : 組織が定めた物理アクセスコントロール・システム/デバイス].- 警備員 <p>];</p> <p>b. 物理アクセス監査ログを維持</p> <p>[設定 : 組織が定めた出入口];</p> <p>c. 次の提供</p> <p>[設定 : 組織が定めたセキュリティ保護手段]</p> <p>施設の中で、公衆のアクセスが可能と指定されたエリアへのアクセスのコントロール</p> <p>d. 訪問者をエスコートし、訪問者の行動を監視</p> <p>[設定 : 訪問者のエスコートと監視が必要と、組織が定めた状況];</p> <p>e. 鍵、コンビネーション、その他の物理アクセスデバイスの保護</p> <p>f. 資産の棚卸</p> <p>[設定 : 組織が定めた物理アクセスデバイス]</p> <p>すべて</p> <p>[設定 : 組織が定めた頻度]; そして</p> <p>g. 組み合わせとキーの変更</p> <p>[設定 : 組織が定めた頻度]</p> <p>その他鍵が紛失した場合、組み合わせが損なわれた場合、または個人の異動や解雇された場合。</p> <p>参照 : FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78, 800-116; ICD 704, 705; DoDI 5200.39; エンタープライズ物理アクセス制御システム (E-PACS)</p>	<p>-----</p> <p>すべての影響レベル :</p> <p>a. 2 CSP が定義した物理アクセスコントロールシステム/デバイスと警備員</p> <p>d. 情報システムが存在する制限されたアクセスエリア内のすべての状況</p> <p>f. 少なくとも年に 1 回</p> <p>g. 少なくとも年に 1 回</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>
--	--

における個人識別認証 (PIV) Web : idmanagement.gov、fips201ep.cio.gov	
PE-3 (1) ; 物理的および環境的防護; 物理的 アクセス制御 - 強化: 情報システムアクセス 組織は、施設の物理的なアクセスコントロー ルに加えて、情報システムへの物理アクセス の許可の強制 [設定: 組織が定めた情報システムのコンポ ーネントを含む物理的空間]; 参照: なし	PE-3 (1) [値は未設定。 CSP により設定される]
PE-4; 物理的および環境的防護; 伝送媒体の アクセス制御: 組織は、 [設定: 組織が定めた情報システムの配電線 および送電線] 組織の施設内で [設定: 組織が定めたセキュリティ保護手 段]; 参照: NSTISSI No. 7003	PE-4 [値は未設定。 CSP により設定される]
PE-6; 物理的および環境的防護; 物理アクセ スの監視: 組織: a. 情報システムが存在する施設への物理アク セスを監視し、物理的なセキュリティインシ デントを検出して対応	PE-6 すべての影響レベル: b. 少なくとも毎月

<p>b. 物理アクセスログのレビュー [設定：組織が定めた頻度] 次の発生時に [設定：組織が定めたイベントやイベント発生の可能性]; そして c. 組織のインシデント・レスポンス機能によるレビューと調査結果の調整</p> <p>参照：なし</p>	<p>根拠：FedRAMP v2 -----</p>
<p>PE-8; 物理的および環境的防護; アクセス記録 RENAMED: 訪問者アクセス記録: 組織: a. 情報システムが存在する施設への訪問者アクセス記録の維持 [設定：組織が定めた期間]; そして b. 訪問者のアクセス記録の確認 [設定：組織が定めた頻度]。</p> <p>参照：なし</p>	<p>PE-8 すべての影響レベル: 最低 1 年間 b. 少なくとも毎月 根拠：FedRAMP v2 -----</p>
<p>PE-10; 物理的および環境的防護; 緊急遮断: 組織: a. 緊急時に情報システムまたは個々のシステムコンポーネントの電源を遮断する機能を提供 b. 次へ緊急遮断スイッチやデバイスの設置 [設定：情報によって組織が定めたシステムまたはシステムコンポーネントの場所] 操作員が安全かつ簡単なアクセス そして c. 許可されていない緊急電源遮断操作の保護</p> <p>参照：なし</p>	<p>PE-10 [値は未設定。 CSP により設定される]</p>

<p>PE-13 (2) ; 物理的および環境的防護; 防火 - 強化: 抑制装置/システム</p> <p>組織は、情報システムのための消火装置/システムを使用して、</p> <p>[設定: 組織が定めた要員または役割]</p> <p>そして</p> <p>[設定: 組織が定めた緊急時対応者].</p> <p>参照: なし</p>	<p>PE-13 (2)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>PE-14; 物理的および環境的防護; 温度と湿度 コントロール:</p> <p>組織:</p> <p>a. 情報システムが所在する施設内の温度と湿度のレベルを維持</p> <p>[設定: 組織が定めた許容レベル].</p> <p>そして</p> <p>b. 温度と湿度のレベルの監視</p> <p>[設定: 組織が定めた頻度].</p> <p>参照: なし</p>	<p>PE-14</p> <p>DoD CSP :</p> <p>注: PE-14 の DoD 値は FedRAMP 値と同等で、業界標準であり、評価の基準である。この値は、DoD がすべての CSP のインフラストラクチャやサービスの提供について定義するのには適切ではない。商用 CSP は FedRAMP 値を使用することができるが、DoD CSP は DoD 値に従わなければならない。</p> <p>DoD CSP 値:</p> <p>a. 商用グレードの情報システムの場合: 64.4~80.6 度 F; 45%~60%相対湿度;露点 41.9° F~59° F; IT 機器筐体の吸気口で測定;他のシステムでは、メーカー仕様内のレベル</p> <p>b. 製造業者の仕様が、制御が必要とされないほど広い公差を許容しない限り、継続的に</p> <p>根拠: DoD RMF TAG</p> <p>-----</p>

	<p>商用 CSP :</p> <p>a. データ処理環境のための熱的ガイドラインと題する米国暖房、冷凍空調技術者協会 (ASHRAE) の文書と一致</p> <p>b. 連続的に</p> <p>根拠 : FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス :</p> <p>PE-14a. 要件 : サービスプロバイダは、サーバーの吸気口で温度と露点による湿度を測定</p>
<p>PE-16; 物理的および環境的防護; 配達と削除 :</p> <p>組織は、認証、監視、および制御</p> <p>[設定 : 組織が定めた情報システムコンポーネントの種類]</p> <p>施設への入退室とそれらの項目の記録を保持</p> <p>参照 : なし</p>	<p>PE-16</p> <p>すべての影響レベル :</p> <p>すべての情報システムコンポーネント</p> <p>根拠 : FedRAMP v2</p>
<p>PE-17; 物理的および環境的防護; 代替サイト :</p> <p>組織 :</p> <p>a. 採用</p> <p>[設定 : 組織が定めたセキュリティ管理策]</p> <p>代替サイトにて</p> <p>b. 代替サイトにおけるセキュリティ管理策の有効性を評価 —そして</p> <p>c. セキュリティインシデントや問題が発生した場合に、従業員が情報セキュリティ担当者と通信するための手段を提供</p>	<p>PE-17</p> <p>[値は未設定。 CSP により設定される]</p>

参照 : NIST Special Publication 800-46	
<p>PL-1; プランニング; セキュリティ計画の方針と手順 :</p> <p>組織 :</p> <p>a. 開発、文書化、配布</p> <p>[設定 : 組織が定めた要員または役割] :</p> <p>1. 目的、範囲、役割、責任、管理コミットメント、組織エンティティ間の調整、コンプライアンスを記述したセキュリティ計画の方針 そして</p> <p>2. セキュリティ計画策定および関連するセキュリティ計画の実施を容易にする手順コントロール;</p> <p>そして</p> <p>b. 現状のレビューと更新 :</p> <p>1. セキュリティ計画の方針</p> <p>[設定 : 組織が定めた頻度] ;</p> <p>そして</p> <p>2. セキュリティ計画の手順</p> <p>[設定 : 組織が定めた頻度].</p> <p>参照 : NIST Special Publications 800-12、800-18、800-100</p>	<p>PL-1</p> <p>影響レベル 4-6 :</p> <p>a. すべての人員</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル :</p> <p>b.1 少なくとも 3 年毎</p> <p>b.2 少なくとも毎年</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>
<p>PL-2; プランニング; システムセキュリティ計画 :</p> <p>組織 :</p> <p>a. 情報システムのセキュリティ計画を策定</p> <p>1. 組織のエンタープライズアーキテクチャとの一貫性</p>	<p>PL-2</p>

<p>2. システムの認可境界を明示的に定義</p> <p>3. ミッションやビジネスプロセスの観点から見た情報システムの運用状況の記述</p> <p>4. 支持根拠を含む情報システムのセキュリティ分類の提供</p> <p>5. 情報システムや関連した接続関係の運用環境の説明</p> <p>6. システムのセキュリティ要件の概要の提供</p> <p>7. 該当する場合は、関連するオーバーレイの識別</p> <p>8. その必要条件を満たすために実施・計画されたセキュリティ管理策と、仕立てと補完の決定理由の説明</p> <p>9. 計画の実施に先立ち、権限のある職員または指定された代表者によるレビューと承認</p> <p>b. セキュリティ計画のコピーの配布と、その後の計画の変更を次へ伝達</p> <p>[設定：組織が定めた要員または役割];</p> <p>c. 情報システムのセキュリティ計画をレビューする</p> <p>[設定：組織が定めた頻度].</p> <p>d. 情報システム/運用環境の変更や計画の実施中またはセキュリティ管理策の評価中に特定された問題に対処するための計画の更新—そして</p> <p>e. 不正な開示や改ざんからセキュリティ計画を保護</p> <p>参照：NIST Special Publication 800-18</p>	<p>影響レベル 4-6：</p> <p>b. 少なくとも ISS0、ISSM、SCA</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル：</p> <p>c. 少なくとも年に 1 回</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
--	--

<p>PL-2 (3) ; プランニング; システムセキュリティ計画 - 強化 : 他の組織との計画/調整</p> <p>組織は、情報システムに影響を及ぼすセキュリティ関連の活動を計画し、調整を実施 [設定 : 組織が定めた個人または団体] 他の組織体への影響を減らすために、そのような活動を行う前に</p> <p>参照 : なし</p>	<p>PL-2 (3)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>PL-4; プランニング; 行動の規則 :</p> <p>組織 :</p> <p>a. 情報や情報システムの使用に関する責任と期待される行動を記述する規則を確立し、情報システムへのアクセスを必要とする要員が容易に利用できるようにする。</p> <p>b. 情報や情報システムへのアクセスを認可する前に、行動規則を読み、理解し、それを遵守することを示した、署名された了承を要員から受け取る。</p> <p>c. レビューし、行動のルールを更新 [設定 : 組織が定めた頻度]。</p> <p>そして</p> <p>d. 行動規則が改訂/更新された場合、前のバージョンの行動規則に署名した要員は、再度の署名が必要</p> <p>参照 : NIST Publication 800-18</p>	<p>PL-4</p> <p>影響レベル 4-6 :</p> <p>c. 毎年</p> <p>根拠 : DoD RMF TAG -----</p> <p>影響レベル 2 :</p> <p>c. 少なくとも 3 年ごと</p> <p>根拠 : FedRAMP v2 -----</p>
<p>PL-8; プランニング; 情報セキュリティアーキテクチャ :</p> <p>組織 :</p>	<p>PL-8</p>

<p>a. 情報システムのための情報セキュリティアーキテクチャの開発</p> <ol style="list-style-type: none"> 1. 組織情報の機密性、完全性、および可用性を保護することに関する全体的な基本姿勢、要件、およびアプローチを記述 2. 情報セキュリティアーキテクチャがエンタープライズアーキテクチャにどのように統合され、サポートされているかを記述 –そして 3. 外部サービスに関する情報セキュリティの前提および外部サービスに対する依存関係について説明 <p>b. 情報セキュリティアーキテクチャのレビューと更新</p> <p>〔設定：組織が定めた頻度〕</p> <p>エンタープライズアーキテクチャの更新を反映 –そして</p> <p>c. 計画された情報セキュリティアーキテクチャの変更が、セキュリティ計画、セキュリティコンセプト（CONOPS）と組織の調達/取得に反映されることを保証</p> <p>参照：なし</p>	<p>すべての影響レベル：</p> <p>b. 少なくとも毎年</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>PL-8 (1) ; プランニング; 情報セキュリティアーキテクチャ - 強化：</p> <p>縦深防護</p> <p>組織は、次のような徹底的な防御アプローチを使用してセキュリティアーキテクチャを設計</p> <p>a. 割り当て</p> <p>〔設定：組織が定めたセキュリティ保護手段〕</p> <p>次について</p>	<p>PL-8 (1)</p> <p>〔値は未設定。 CSP により設定される〕</p>

<p>[設定：組織が定めた場所とアーキテクチャ];</p> <p>そして</p> <p>b. 割り当てられたセキュリティ措置が、連携し相互補強的に機能することを確保</p> <p>参照：なし</p>	
<p>PS-1; 人的セキュリティ; 要員のセキュリティ方針と手続き:</p> <p>組織:</p> <p>a. 開発、文書化、配布</p> <p>[設定：組織が定めた要員または役割]:</p> <p>1. 目的、範囲、役割、責任、管理コミットメント、組織エンティティ間の調整、コンプライアンスを記述した要員のセキュリティ方針—そして</p> <p>2. 要員のセキュリティ方針や関連のセキュリティ管理策の円滑な遂行のための手順—そして</p> <p>b. 現状のレビューと更新:</p> <p>1. 要員のセキュリティポリシー</p> <p>[設定：組織が定めた頻度];</p> <p>2. 要員のセキュリティ手続き</p> <p>[設定：組織が定めた頻度].</p> <p>参照：なし</p>	<p>PS-1</p> <p>影響レベル 4-6:</p> <p>a. すべての人員</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル:</p> <p>b. 1 少なくとも 3 年ごと</p> <p>b. 2 少なくとも年に 1 回</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>PS-2; 人的セキュリティ; 役職の分類</p> <p>RENAMED: 役職のリスク指定:</p> <p>組織:</p> <p>a. すべての組織の役職へリスク指定を割当</p> <p>b. これらの役職を満たす個人のスクリーニング基準を設定 — そして</p> <p>c. ポジションリスク指定のレビューと更新</p>	<p>PS-2</p> <p>影響レベル 4-6:</p> <p>c. 毎年</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>

<p>[設定：組織が定めた頻度].</p> <p>参照：なし</p>	<p>影響レベル 2：</p> <p>c. 少なくとも 3 年ごと</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>PS-3；人的セキュリティ；人材スクリーニング：</p> <p>組織：</p> <p>a. 情報システムへのアクセスを許可する前の個人のスクリーニング – そして</p> <p>b. 個人の再スクリーニング</p> <p>[設定：組織が定めた再スクリーニングが必要な条件、再スクリーニングが記載されている場合の頻度].</p> <p>参照：なし</p>	<p>PS-3</p> <p>すべての影響レベル：</p> <p>国家セキュリティクリアランス；機密のセキュリティクリアランス 5 年目；極秘セキュリティクリアランスの 10 年目；秘密のセキュリティクリアランス 15 年目に再審査が必要</p> <p>中程度のリスクの法執行と高影響度の public trust level については、5 年目に再審査が必要。その他の中程度のリスク職位と低いリスク職位についての再審査はない。</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>PS-3 (3)；人的セキュリティ；人材スクリーニング – 強化：</p> <p>特別保護措置に関する情報</p> <p>組織は、特別な保護を必要とする情報を処理、保管、または送信する情報システムにアクセスする個人について、以下を確実に実施</p> <p>a. 正式な政府の職務職権で示された有効なアクセス権限を有すること。そして</p> <p>b. 以下を満たす</p> <p>[設定：組織が定めた追加のスクリーニング基準].</p> <p>参照：なし</p>	<p>PS-3 (3)</p> <p>すべての影響レベル：</p> <p>b. 個人のスクリーニング基準 – 特定の情報によって必要とされる。</p> <p>根拠：FedRAMP v2</p> <p>-----</p>

<p>PS-4; 人的セキュリティ; 人事解雇 :</p> <p>組織は、個々の雇用の終了時に :</p> <p>a. 情報システムへのアクセス無効化 [設定 : 組織が定めた時間];</p> <p>b. 個人に関連する認証/資格情報の停止/取消</p> <p>c. 以下の質疑を含む退職時の面接の実施 [設定 : 組織が定めた情報セキュリティの話題];</p> <p>d. セキュリティに関連した組織の情報、システム関連のプロパティのすべての取戻し</p> <p>e. 停止した個人に管理されていた組織情報および情報システムへのアクセスの保持。そして</p> <p>f. 次へ通知 [設定 : 組織が定めた要員または役割] 以内 [設定 : 組織が定めた期間].</p> <p>参照 : NIST Special Publication 800-35</p>	<p>PS-4</p> <p>影響レベル 4-6 :</p> <p>a. 終了時にアカウントの無効化を調整できない場合は、8 時間</p> <p>f. 最低限、ISSO と資格を取り消す責任がある担当者</p> <p>f. 直ちにまたは 24 時間以内に</p> <p>根拠 : DoD RMF TAG (a. FedRAMP 高ベースライン WG)</p> <p>-----</p> <p>影響レベル 2 :</p> <p>a. 同日</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>
<p>PS-5; 人的セキュリティ; 人事異動 :</p> <p>組織 :</p> <p>a. 個人が組織内の他の職に再割り当てまたは移転された場合に、情報システム/施設に対する現在の論理的アクセスおよび物理的アクセスの認可の継続的な運用上の必要性を検討し、確認する。</p> <p>b. イニシエイト [割当 : 組織が定めた移転または再割当] 以内 [設定 : 組織が定めた正式な移転に続く期間].</p>	<p>PS-5</p> <p>影響レベル 4-6 :</p> <p>b. 不要になったすべてのシステムアクセスが確実に削除する処置</p> <p>b. 異動時にアカウントの無効化を調整できない場合は 24 時間</p> <p>d. 最低限、ISSO と資格の移転を担当する担当者</p> <p>d. 24 時間</p>

<p>c. 再割り当てまたは転送による運用ニーズの変化に対応するために、必要に応じてアクセス許可の変更。－そして</p> <p>d. 通知する</p> <p>[設定：組織が定めた要員または役割] 以内</p> <p>[設定：組織が定めた期間].</p> <p>参照：FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.</p>	<p>根拠：DoD RMF TAG (b. FedRAMP 高ベースライン WG)</p> <p>-----</p> <p>影響レベル 2：</p> <p>c. 正式な異動行為から 24 時間以内に</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>PS-6; 人的セキュリティ; アクセス同意：</p> <p>組織：</p> <p>a. 組織の情報システムのアクセス同意を作成し文書化</p> <p>b. アクセス同意のレビューと更新</p> <p>[設定：組織が定めた頻度].</p> <p>そして</p> <p>c. 組織の情報・情報システムへのアクセスを必要とする要員について、確実に以下を実施</p> <ol style="list-style-type: none">1. アクセスが許可される前に適切なアクセス同意書に署名。そして2. アクセスの同意が更新された場合や次の頻度で、組織の情報システムへのアクセスを維持するためにアクセス合意書へ再度署名 <p>[設定：組織が定めた頻度].</p> <p>参照：OMB 覚書 04-04; NIST Special Publication 800-30、800-39; Web : idmanagement.gov</p>	<p>PS-6</p> <p>影響レベル 4-6：</p> <p>c (2) ユーザのアクセスレベルが変更された場合、少なくとも毎年</p> <p>根拠：DoD RMF TAG と FedRAMP v2</p> <p>-----</p> <p>すべての影響レベル：</p> <p>b. 少なくとも年に 1 回</p> <p>影響レベル 2：</p> <p>c. 2. [少なくとも年に 1 回]</p> <p>根拠：FedRAMP v2</p> <p>-----</p>

<p>PS-7; 人的セキュリティ; サードパーティの要員セキュリティ:</p> <p>組織:</p> <p>a. サードパーティプロバイダーのセキュリティの役割と責任を含む要員のセキュリティ要件を確立</p> <p>b. サードパーティプロバイダーは、組織が設定した要員セキュリティの方針と手続きを遵守する必要がある。</p> <p>c. 要員のセキュリティ要件の文書化</p> <p>d. サードパーティプロバイダーは、以下へ通知する必要がある。</p> <p>[設定: 組織が定めた要員または役割]</p> <p>組織の認証やバッジを所有、またはその内の情報システムの権限を有するサードパーティ要員の異動、取消の場合。</p> <p>[設定: 組織が定めた期間];</p> <p>そして</p> <p>e. プロバイダーのコンプライアンスを監視</p> <p>参照: なし</p>	<p>PS-7</p> <p>影響レベル 4-6:</p> <p>d. 最低限、ISS0 と資格移転の担当者</p> <p>d. 異動または取消にアカウントの無効化を調整できない場合は 24 時間</p> <p>根拠: DoD RMF TAG (d. FedRAMP 高ベースライン WG)</p> <p>-----</p> <p>影響レベル 2:</p> <p>d. 組織が定めた期間 - 同日</p> <p>根拠: FedRAMP v2</p> <p>-----</p>
<p>PS-8; 人的セキュリティ; 人事処分:</p> <p>組織:</p> <p>a. 確立された情報セキュリティ方針と手順に従わない個人に対して、正式な処分プロセスの採用。そして</p> <p>b. 通知</p> <p>[設定: 組織が定めた要員または役割]</p> <p>以内</p> <p>[割当: 組織が定めた期間]</p> <p>要員に対する正式な処分プロセスが開始されたとき、処分を受けた個人とその処分理由の明確化</p> <p>参照: なし</p>	<p>PS-8</p> <p>影響レベル 4-6:</p> <p>b. 少なくとも、ISS0</p> <p>b. 直ちに</p> <p>根拠: DoD RMF TAG</p> <p>-----</p>

<p>RA-1; リスクアセスメント; リスクアセスメントの方針と手順:</p> <p>組織:</p> <p>a. 開発、文書化、配布</p> <p>[設定: 組織が定めた要員または役割]:</p> <ol style="list-style-type: none"> 1. 目的、範囲、役割、責任、管理コミットメント、組織エンティティ間の調整、コンプライアンスを記述したリスクアセスメントの方針 そして 2. リスクアセスメントの方針と関連するリスクアセスメントコントロールの実施を促進するための手順 <p>そして</p> <p>b. 現状のレビューと更新:</p> <ol style="list-style-type: none"> 1. リスクアセスメントの方針 <p>[設定: 組織が定めた頻度];</p> <p>そして</p> <ol style="list-style-type: none"> 2. リスク評価手順 <p>[設定: 組織が定めた頻度].</p> <p>参照: なし</p>	<p>RA-1</p> <p>影響レベル 4-6:</p> <p>a. 少なくとも、ISSM と ISSO</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル:</p> <p>b.1 少なくとも 3 年ごと</p> <p>b.2 少なくとも年に 1 回</p> <p>根拠: FedRAMP v2</p> <p>-----</p>
<p>RA-3; リスクアセスメント; リスクアセスメント:</p> <p>組織:</p> <p>a. 情報システムの不正アクセス、使用、開示、混乱、改変、破壊、その処理、保管、または送信する情報からの危険性の査定、災害の可能性を含むリスクのアセスメントの実施</p> <p>b. リスク評価の結果を文書化</p> <p>[選択:</p> <ul style="list-style-type: none"> - セキュリティ計画; - リスクアセスメント報告書; - [設定: 組織定義文書] <p>];</p>	<p>RA-3</p> <p>影響レベル 4-6:</p> <p>d. ISSM, ISSO, A0 および PM</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル:</p> <p>b. セキュリティアセスメントレポート</p>

<p>c. リスクアセスメント結果のレビュー [設定：組織が定めた頻度]；</p> <p>d. リスクアセスメントの結果の配布 [設定：組織が定めた要員または役割]；そして</p> <p>e. リスクアセスメントの更新する [設定：組織が定めた頻度]</p> <p>情報システムや運用環境（新しい脅威や脆弱性の特定を含む）やシステムのセキュリティ状態に影響を与える可能性があり、または、その他の条件に重大な変更があった場合</p> <p>参照：なし</p>	<p>c. 少なくとも 3 年ごとまたは大幅な変更が発生した場合</p> <p>e. 少なくとも 3 年ごとまたは大幅な変更が発生した場合</p> <p>根拠：FedRAMP v2 -----</p> <p>FedRAMP 追加要件とガイダンス： ガイダンス：重要な変更は、NIST Special Publication 800-37 Revision 1、付録 F に定義されている。</p> <p>RA-3d. 要件：認定担当官を含める； FedRAMP を含む JAB 認可</p>
<p>RA-5；リスクアセスメント；脆弱性スキャン：</p> <p>組織：</p> <p>a. 情報システムとホストされたアプリケーションの脆弱性スキャン [設定：組織が定めたプロセスに従い、その頻度またはランダムに実施]</p> <p>潜在的にシステム/アプリケーションに影響を与える新しい脆弱性が特定され報告された場合；</p> <p>b. 以下の基準を使用して、ツール間の相互運用性を高め、脆弱性管理プロセスの一部を自動化する脆弱性スキャンツールや技術の採用</p> <ol style="list-style-type: none"> 1. プラットフォーム、ソフトウェアの欠陥、不適切な構成の列挙。 2. チェックリストとテスト手順の書式設定。そして 3. 脆弱性の影響の測定 	<p>RA-5</p> <p>影響レベル 4-6：</p> <p>a. 30 日ごとまたは信頼できる情報源（IAVM、CTO、DTM、STIG など）の指示に従う。</p> <p>d. 信頼できる情報源（IAVM、CTO、DTM など）に従う、またはハイリスクの脆弱性発見日から 30 日以内に緩和、または中程度のリスクの場合は発見から 90 日以内に緩和。</p> <p>e. 少なくとも、ISSM と ISSO</p> <p>根拠：DoD RMF TAG と FedRAMP v2 -----</p>

<p>c. 脆弱性スキャンレポートとセキュリティ管理策アセスメントの結果の分析</p> <p>d. 脆弱性の是正</p> <p>〔設定：組織が定めた応答時間〕</p> <p>組織のリスクのアセスメントに従って；そして</p> <p>e. 脆弱性スキャンプロセスやセキュリティ管理策評価から得られた情報を以下で共有</p> <p>〔設定：組織が定めた要員または役割〕</p> <p>他の情報システムにおける類似の脆弱性（すなわち、システムの弱点または欠点）を排除するのに役立てる。</p> <p>参照：なし</p>	<p>影響レベル 2：</p> <p>オペレーティングシステム/インフラは毎月；Web アプリケーションとデータベースは毎月</p> <p>d. 高レベルのリスクは発見日から 30 日以内に緩和；または中程度のリスクの場合は発見から 90 日以内に緩和。</p> <p>根拠：FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>RA-5a. 要件：認定された独立した評価担当者により、年 1 回オペレーティングシステム/インフラストラクチャ、Web アプリケーションやデータベースをスキャン</p> <p>RA-5e. 要件：リスクエグゼクティブを含める。 または FedRAMP を含む JAB 認可</p>
<p>RA-5 (2)；リスクアセスメント；脆弱性スキャン - 強化：</p> <p>頻度別/新しいスキャン前/発見時に更新</p> <p>組織は、スキャンした情報システムの脆弱性を更新</p> <p>〔選択（1 つまたは複数）：</p> <ul style="list-style-type: none">- 〔設定：組織が定めた頻度〕；- 新しいスキャンの前に；- 新しい脆弱性が特定され、報告されたとき。 <p>〕.</p> <p>参照：なし</p>	<p>RA-5 (2)</p> <p>すべての影響レベル：</p> <p>新しいスキャンの前に</p> <p>根拠：FedRAMP v2</p> <p>-----</p>

<p>RA-5 (5) ; リスクアセスメント; 脆弱性スキャン – 強化 : 特権アクセス</p> <p>情報システムは、次へ特権アクセス許可を実装</p> <p>[設定 : 組織が特定した情報システムコンポーネント]</p> <p>選択された対象について</p> <p>[設定 : 組織が定めた脆弱性スキャン].</p> <p>参照 : NIST Special Publication 800-65</p>	<p>RA-5 (5)</p> <p>影響レベル 4-6 : すべての情報システムとインフラストラクチャコンポーネント</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2 : オペレーティングシステム/Web アプリケーション/データベース</p> <p>すべてのスキャン</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>
<p>SA-1; システムとサービスの取得; システムとサービスの取得方針と手順 :</p> <p>組織 :</p> <p>a. 開発、文書化、配布</p> <p>[設定 : 組織が定めた要員または役割] :</p> <ol style="list-style-type: none"> 1. 目的、範囲、役割、責任、管理、コミットメント、組織間の調整、コンプライアンスを記述したシステムやサービスの取得方針—そして 2. システムやサービスの取得方針の実施を促進するための手順とその取得コントロール。 <p>そして</p> <p>b. 現状のレビューと更新 :</p> <ol style="list-style-type: none"> 1. システムおよびサービスの取得ポリシー 	<p>SA-1</p> <p>影響レベル 4-6 : a. すべての人員</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル : b. 1 少なくとも 3 年ごと b. 2 少なくとも年に 1 回</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>

<p>[設定：組織が定めた頻度]； そして 2. システムおよびサービスの取得手順 [設定：組織が定めた頻度].</p> <p>参照：なし</p>	
<p>SA-3；システムとサービスの取得；ライフサイクルサポート RENAMED：システム開発ライフサイクル：</p> <p>組織：</p> <p>a. 以下を利用した情報システムの管理 [設定：組織が定めたシステム開発のライフサイクル]</p> <p>情報セキュリティ考慮事項の組み込み</p> <p>b. システム開発のライフサイクルを通じて情報セキュリティの役割と責任を定義し文書化 c. 情報セキュリティの役割と責任を持つ個人を指定—そして d. 組織の情報セキュリティリスク管理プロセスをシステム開発のライフサイクル活動に統合</p> <p>参照：なし</p>	<p>SA-3</p> <p>[値は未設定。 CSP により設定される]</p>
<p>SA-4 (2) ； システムとサービスの取得；取得 RENAMED：取得プロセス – 強化： セキュリティ管理策の設計/実装情報</p> <p>組織は、情報システム、システムコンポーネントや情報システムサービスの開発者に、以下を含む採用されるセキュリティ管理策の設計情報と実装情報の提供を要求</p> <p>[選択 (1 つまたは複数)：</p> <p>– セキュリティ関連の外部システムインターフェース；</p>	<p>SA-4 (2)</p> <p>すべての影響レベル：</p> <p>セキュリティ関連の外部システムインターフェースと高水準設計を含める。</p> <p>根拠：FedRAMP v2</p> <p>-----</p>

<ul style="list-style-type: none"> - 高レベルな設計； - 低レベルな設計； - ソースコードまたはハードウェア回路図； - [設定：組織が定めた設計/実装情報] <p>次により</p> <p>[設定：組織が定めた詳細レベル].</p> <p>参照：なし</p>	
<p>SA-4 (8)；システムとサービスの取得；取得プロセス - 強化：</p> <p>継続的なモニタリング計画</p> <p>組織は、情報システム、システムコンポーネントや情報システムサービスの開発者に対し、セキュリティ管理策の有効性を継続的に監視する計画の策定を要求</p> <p>[設定：組織が定めた詳細レベル].</p> <p>参照：なし</p>	<p>SA-4 (8)</p> <p>すべての影響レベル：</p> <p>少なくともコントロール CA-7 に定義されている最小要件</p> <p>根拠：FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>SA-4 (8) ガイダンス：CSP は、システムコンポーネントや情報システムサービスの取得場所にかかわらず、同じセキュリティ基準を使用する必要がある。</p>
<p>SA-5;システムとサービスの取得;情報システムのドキュメント：</p> <p>組織：</p> <p>a. 以下を説明する情報システム、システムコンポーネントや情報システムサービスの管理者用マニュアルの入手</p> <p>1. システム、コンポーネント、またはサービスのセキュアな構成、インストールと操作。</p>	<p>SA-5</p> <p>影響レベル 4-6：</p> <p>e. 少なくとも、ISSO、ISSM、および SCA</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>

<p>2. セキュリティ機能/メカニズムの効果的な使用と維持;そして</p> <p>3. 管理（すなわち特権）機能の構成と使用に関する既知の脆弱性。</p> <p>b. 以下を記述した情報システム、システムコンポーネントや情報システムサービスの利用者マニュアルを入手</p> <p>1. 利用者がアクセス可能なセキュリティ機能/メカニズムやこれらのセキュリティを効果的に使用する方法</p> <p>2. システム、コンポーネントやサービスをより安全に利用する際の操作方法—そして</p> <p>3. システム、コンポーネントやサービスのセキュリティを維持するためのユーザの責任</p> <p>c. 情報システム、システムコンポーネントについて、そのような文書が利用できない、または存在しない場合</p> <p>〔設定：組織が定めたアクション〕</p> <p>に応じて;</p> <p>d. リスク管理戦略に従って、必要に応じて文書を保護—そして</p> <p>e. ドキュメントを次へ配布</p> <p>〔設定：組織が定めた要員または役割〕.</p> <p>参照：なし</p>	
<p>SA-9; システムとサービスの取得; 外部情報システムサービス:</p> <p>組織:</p> <p>a. 外部情報システムサービスの提供者は、組織の情報セキュリティ要件を遵守し、</p> <p>〔設定：組織が定めたセキュリティ管理策〕</p>	<p>SA-9</p> <p>影響レベル 4-6:</p> <p>a. CNSSI 1253 および FedRAMP Security Controls Baseline (s) によって定義されたセキュリティ管理策</p>

<p>適用される連邦法、大統領令、指令、方針、規制、基準、指針に従って、</p> <p>b. 外部情報システムサービスに関する政府の監督とユーザの役割と責任を定義し文書化 –そして</p> <p>c. 実施</p> <p>〔設定：組織が定めたプロセス、方法や技術〕</p> <p>外部サービスプロバイダによるセキュリティ管理策コンプライアンスの継続的な監視</p> <p>参照：なし</p>	<p>根拠：DoD RMF TAG と FedRAMP v2</p> <p>-----</p> <p>影響レベル 2：</p> <p>a. 連邦の情報が外部システム内で処理または格納されている場合は、FedRAMP のセキュリティ管理策のベースライン</p> <p>すべての影響レベル：</p> <p>c. 連邦の情報が処理または格納されている外部システムでは連邦/FedRAMP の継続的な監視の要件を満たす必要がある。</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>SA-9 (1)；システムとサービスの取得；外部情報システムサービス – 強化：</p> <p>リスクアセスメント/組織の承認</p> <p>組織：</p> <p>a. 専任の情報セキュリティサービスの取得またはアウトソーシングに先立ち、リスクについて組織の評価を実施 –そして</p> <p>b. 専用の情報セキュリティサービスの取得や外部委託について次による承認を得る</p> <p>〔設定：組織が定めた要員または役割〕.</p> <p>参照：なし</p>	<p>SA-9 (1)</p> <p>影響レベル 4-6：</p> <p>b. DoD コンポーネント CIO またはその代表者</p> <p>根拠：</p> <p>DoD の RMF TAG</p> <p>-----</p> <p>影響レベル 2：</p> <p>追加要件とガイダンスを参照</p> <p>根拠：FedRAMP v2</p> <p>-----</p>

	<p>FedRAMP 追加要件とガイダンス：</p> <p>SA-9 (1) . 要件：サービスプロバイダは、既存のアウトソーシングされたセキュリティサービスをすべて文書化し、将来アウトソーシングされるセキュリティサービスのリスクアセスメントを実施する。JABの認可については、今後予定されている委託されたサービスが承認され、JABに受理される。</p>
<p>SA-9 (2) ; システムとサービスの取得; 外部情報システム - 強化:</p> <p>機能/ポート/プロトコル/サービスの識別</p> <p>組織は、プロバイダへ次を要求</p> <p>〔設定：組織が定めた外部の情報システムサービス〕</p> <p>そのようなサービスの利用に必要な機能、ポート、プロトコルやその他のサービスを識別</p> <p>参照：なし</p>	<p>SA-9 (2)</p> <p>すべての影響レベル：</p> <p>連邦の情報が処理、送信、または保管されるすべての外部システム</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>SA-9 (4) ; システムとサービスの取得; 外部情報システム - 強化:</p> <p>利用者とプロバイダの一貫した関心事項</p> <p>組織は、次を実施</p> <p>〔設定：組織が定めたセキュリティ保護手段〕</p> <p>次への関心事項を確実化</p> <p>〔設定：組織が定めた外部サービスプロバイダ〕</p> <p>組織の関心事項を反映し一貫性を維持</p> <p>参照：なし</p>	<p>SA-9 (4)</p> <p>すべての影響レベル：</p> <p>連邦の情報が処理、送信、または保管されるすべての外部システム</p> <p>根拠：FedRAMP v2</p> <p>-----</p>

<p>SA-9 (5) ; システムとサービスの取得; 外部 情報システム - 強化: ストレージとサービスの場所の処理</p> <p>組織は、</p> <p>[選択 (1 つまたは複数):</p> <ul style="list-style-type: none">- 情報処理;- 情報/データ ;- 情報システムサービス <p>]</p> <p>次について</p> <p>[設定 : 組織が定めた場所]</p> <p>次に基いて</p> <p>[設定 : 組織が定めた要件または条件].</p> <p>参照 : ISO / IEC 15408; NIST Special Publication 800-53A; ウェブ : nvd.nist.gov、cwe.mitre.org、 cve.mitre.org、capec.mitre.org</p>	<p>SA-9 (5)</p> <p>すべての影響レベル :</p> <p>情報処理、伝送、情報データや情報サービス</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>
<p>SA-10; システムとサービスの取得; 開発者の 構成管理 :</p> <p>組織は、情報システム、システムコンポーネ ントや情報システムサービスの開発者に以下 を要求</p> <p>a. システム、コンポーネントやサービスに対 し構成管理を実行</p> <p>[選択 (1 つまたは複数):</p> <ul style="list-style-type: none">- 設計;- 開発;- 実装;- 運用 <p>];</p> <p>b. 変更の整合性を文書化し、管理し、制御す る。</p>	<p>SA-10</p> <p>影響レベル 4-6 :</p> <p>e. 少なくとも、ISSO と ISSM</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル :</p> <p>a. 開発、実装、および運用</p> <p>根拠 : FedRAMP v2</p> <p>-----</p> <p>FedRAMP 追加要件とガイダンス :</p>

<p>[設定：組織が定めた構成管理下の構成項目];</p> <p>c. 組織が承認した変更のみをシステム、コンポーネント、またはサービスに実装する。</p> <p>d. システム、コンポーネント、またはサービスへの承認された変更、その変更による潜在的なセキュリティへの影響の文書化; そして</p> <p>e. システム、コンポーネント、またはサービス内のセキュリティ上の欠陥と欠陥の修正を追跡し、調査結果を報告</p> <p>[設定：組織が定めた要員].</p> <p>参照：なし</p>	<p>SA-10e. 要件：JAB の認可では、システム、コンポーネント、またはサービス内のセキュリティ上の欠陥と欠陥解決を追跡し、組織が定めた FedRAMP を含む担当者へ調査結果を報告</p>
<p>SA-11; システムとサービスの取得; 開発者のセキュリティテスト</p> <p>RENAMED：開発者のセキュリティテストと評価:</p> <p>組織は、情報システム、システムコンポーネントや情報システムサービスの開発者に以下を要求</p> <p>a. セキュリティアセスメント計画を作成して実装</p> <p>b. 以下の実行</p> <p>[選択 (1 つまたは複数) :</p> <ul style="list-style-type: none"> - 単位; - 統合; - システム; - リグレーション <p>]</p> <p>テスト/評価</p> <p>[設定：組織が定めた深度とカバレッジ];</p> <p>c. セキュリティアセスメント計画の実行とセキュリティテスト/評価の結果の証拠を生成する。</p>	<p>SA-11</p> <p>すべての影響レベル:</p> <p>b. ユニット、統合; システム; リグレーション</p> <p>インフラストラクチャーレベル</p> <p>根拠：DoD ベストプラクティス</p> <p>-----</p>

<p>d. 検証可能な欠陥修正プロセスを実装</p> <p>e. セキュリティテスト/評価中に特定された欠陥を修正</p> <p>参照：なし</p>	
<p>SA-12；システムとサービスの取得；サプライチェーンの保護：</p> <p>組織は、情報システム、システムコンポーネントや情報システムサービスに対するサプライチェーンの脅威から保護</p> <p>[設定：組織が定めたセキュリティ保護手段]</p> <p>包括的で縦深防護情報セキュリティ戦略の一環として、</p> <p>参照：なし</p>	<p>SA-12</p> <p>影響レベル 5-6：</p> <p>DoD 5200.44 「信頼できるシステムとネットワーク（TSN）を達成するためのミッションクリティカルな機能の保護」</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>
<p>SA-19；システムとサービスの取得；コンポーネントの真正性：</p> <p>組織：</p> <p>a. 偽造品の情報システムへの侵入の検出と防止手段を含む偽造防止方針と手順を開発し、実施する。そして</p> <p>b. 偽造情報システムのコンポーネントの報告</p> <p>[選択（1つまたは複数）：</p> <ul style="list-style-type: none">- 偽造品の供給源；- [設定：組織が定めた外部報告組織]；- [設定：組織が定めた要員または役割] <p>].</p> <p>参照：なし</p>	<p>SA-19</p> <p>影響レベル 5-6：</p> <p>b. 少なくとも、USCYBERCOM</p> <p>b. 少なくとも、ISSO、ISSM、および PM</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>

<p>SC-1; システムと通信の保護; システムと通信の保護方針と手順:</p> <p>組織:</p> <p>a. 開発、文書化、配布</p> <p>[設定: 組織が定めた要員または役割]:</p> <p>1. 目的、範囲、役割、責任、経営者のコミットメント、組織間の調整、コンプライアンスを記述したシステムと通信保護の方針</p> <p>2. システムと通信保護の方針と関連するシステムと通信の保護コントロールの実行を促進するための手続</p> <p>そして</p> <p>b. 現状のレビューと更新:</p> <p>1. システムおよび通信保護ポリシー</p> <p>[設定: 組織が定めた頻度]; そして</p> <p>2. システムおよび通信の保護手順</p> <p>[設定: 組織が定めた頻度].</p> <p>参照: なし</p>	<p>SC-1</p> <p>影響レベル 4-6:</p> <p>a. 少なくとも、ISSM/ISSO</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル:</p> <p>b.1 少なくとも 3 年ごと</p> <p>b.2 少なくとも年に 2 回</p> <p>根拠: FedRAMP v2</p> <p>-----</p>
<p>SC-5; システムと通信の保護; サービス拒否の保護:</p> <p>情報システムは、次のタイプのサービス拒否攻撃の影響を防止または制限</p> <p>[設定: 組織が定めたサービス拒否攻撃の種類や、そのような情報の参照元]</p> <p>次を実行して</p> <p>[設定: 組織が定めたセキュリティ保護手段].</p> <p>参照: なし</p>	<p>SC-5</p> <p>[値は未設定。 CSP により設定される]</p>

<p>SC-6; システムと通信の保護; リソースの優先順位</p> <p>RENAMED: リソースの可用性:</p> <p>情報システムは、リソースの可用性を確保するために、次を割当</p> <p>[設定: 組織が定めたリソース]</p> <p>次の手段で</p> <p>[選択 (1 つまたは複数)];</p> <ul style="list-style-type: none">- 優先度;- クォータ;- [設定: 組織が定めたセキュリティ保護手段] <p>].</p> <p>参照: なし</p>	<p>SC-6</p> <p>[値は未設定。 CSP により設定される]</p>
<p>SC-7 (4); システムと通信の保護; 境界保護 - 強化:</p> <p>外部電気通信サービス</p> <p>組織:</p> <p>a. 各々の外部電気通信サービスにおける管理インターフェースの実装</p> <p>b. 管理対象インターフェースごとにトラフィックフローポリシーの確立</p> <p>c. 各インターフェースを介して送信される情報の機密性と完全性の保護</p> <p>d. 必要な支援ミッション/ビジネスニーズと持続時間を備えたトラフィックフローポリシーの例外の文書化 - そして</p> <p>e. トラフィックフローポリシーに対する例外のレビュー</p> <p>[設定: 組織が定めた頻度]</p> <p>ミッション/ビジネスニーズの明確な裏付けがない例外の削除</p>	<p>SC-7 (4)</p> <p>影響レベル 4-6:</p> <p>e. 180 日ごと</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2:</p> <p>e. 少なくとも年に 1 回</p> <p>根拠: FedRAMP v2</p> <p>-----</p>

参照：なし	
<p>SC-7 (8) ; システムと通信の保護; 境界保護 - 強化:</p> <p>認証付きプロキシサーバーへのトラフィックのルーティング</p> <p>情報システムルート</p> <p>[設定：組織が定めた内部コミュニケーショントラフィック]</p> <p>次に対し</p> <p>[設定：組織が定めた外部ネットワーク]</p> <p>管理されたインターフェースで認証されたプロキシサーバーを使用</p> <p>参照：なし</p>	<p>SC-7 (8)</p> <p>影響レベル 4-6 :</p> <p>PPSM ガイダンス (HTTPS、HTTP、FTP、SNMP など) によって指定されたプロトコル</p> <p>認可境界の外部のネットワーク</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>
<p>SC-7 (11) ; システムと通信の保護; 境界保護 - 強化:</p> <p>着信通信トラフィックの制限</p> <p>情報システムは、次からの通信だけを許可</p> <p>[設定：組織が定めた認可された情報源]</p> <p>次の経路</p> <p>[設定：組織が定めた許可された宛先]</p> <p>参照：なし</p>	<p>SC-7 (11)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>SC-7 (12) ; システムと通信の保護; 境界保護 - 強化:</p> <p>ホストベースの保護</p> <p>組織は、次を実装</p> <p>[設定：組織が定めたホストベースの境界保護メカニズム]</p>	<p>SC-7 (12)</p> <p>影響レベル 4-6 :</p> <p>ホスト侵入防止システム (HIPS)</p> <p>すべての情報システムコンポーネント。</p>

<p>次について</p> <p>[設定：組織が定めた情報システムコンポーネント].</p> <p>参照：なし</p>	<p>根拠：DoD RMF TAG</p> <p>-----</p> <p>注：DISA は、商用 CSP との同等性をケースバイケースで評価</p>
<p>SC-7 (13) ; システムと通信の保護; 境界保護 - 強化:</p> <p>セキュリティツール/メカニズム/サポートコンポーネントの分離</p> <p>組織は、次を分離</p> <p>[設定：組織が定めた情報セキュリティツール、メカニズム、サポートコンポーネント]</p> <p>システムの他のコンポーネントへの管理されたインターフェースを持つ物理的に別個のサブネットワークを実装することによって、他の内部情報システムコンポーネントから分離</p> <p>参照：なし</p>	<p>SC-7 (13)</p> <p>影響レベル 4-6：</p> <p>PKI、パッチ・インフラストラクチャ、HBSS、サイバーセキュリティ防御ツール、特別目的のゲートウェイ、脆弱性追跡システム、ハニーポット、インターネットアクセスポイント (IAP) ; ネットワーク要素とデータセンターの管理トラフィック ; 非武装地帯 (DMZ)、サーバーファーム/コンピューティングセンター、集中型監査ログサーバーなどのような主要な情報セキュリティツール、メカニズム、サポートコンポーネント。</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2：</p> <p>FedRAMP 追加要件とガイダンス：</p> <p>SC-7 (13) . 要件：サービスプロバイダは、システムやセキュリティ管理策に関連する重要な情報セキュリティツール、メカニズム、およびサポートコンポーネントを定義し、これらのツール、メカニズム、およびサポートコンポーネントを、物理的または論理的に別個のサブネットを介して他の内部情報システムコンポーネントから分離する。</p>

<p>SC-7 (14) ; システムと通信の保護; 境界保護 - 強化:</p> <p>許可されていない物理接続からの保護</p> <p>組織は、次の場所での不正な物理的接続から保護</p> <p>[設定: 組織が定めた管理インターフェース].</p> <p>参照: なし</p>	<p>SC-7 (14)</p> <p>影響レベル 4-6 :</p> <p>インターネットアクセスポイント、LAN から WAN へのエンクレープ、クロスドメインソリューション、DoD 認定の代替ゲートウェイ</p> <p>根拠: DoD RMF TAG</p> <p>-----</p>
<p>SC-8 (1) ; システムと通信の保護; 伝送の完全性</p> <p>RENAMED: 伝送の機密性と完全性 - 強化:</p> <p>暗号または代替の物理的保護</p> <p>情報システムは、暗号メカニズムを実装</p> <p>[選択 (1 つまたは複数):</p> <ul style="list-style-type: none"> - 情報の不正な開示の防止; - 情報改ざんの検出; <p>]</p> <p>他に保護されていない限り、送信中</p> <p>[設定: 組織が定めた代替物理的安全処置].</p> <p>参照: なし</p>	<p>SC-8 (1)</p> <p>すべての影響レベル:</p> <p>情報の不正な開示を防ぎ、情報の改ざんを検出</p> <p>堅牢化または警告を実装したキャリア保護分配システム (PDS:Protective Distribution Ststem)</p> <p>根拠: FedRAMP v2</p> <p>-----</p>
<p>SC-8 (2) ; システムと通信の保護; 伝送の完全性</p> <p>RENAMED: 伝送の機密性と完全性 - 強化:</p> <p>送信前/送信後の処理</p> <p>情報システムは、次を維持</p> <p>[選択 (1 つまたは複数):</p> <ul style="list-style-type: none"> - 機密性; - 完全性 <p>]</p> <p>送信準備中や受信中の情報</p> <p>参照: なし</p>	<p>SC-8 (2) ;</p> <p>影響レベル 4-6 :</p> <p>機密性と完全性</p> <p>根拠: CNSSI 1253</p> <p>-----</p>

<p>SC-10; システムと通信の保護; ネットワーク切断:</p> <p>情報システムは、セッションの終了時またはその後に通信セッションに関連したネットワーク接続を切断する。</p> <p>[設定: 組織が定めた非活動期間]</p> <p>参照: なし</p>	<p>SC-10</p> <p>影響レベル 4-6:</p> <p>特権セッションは 10 分、ユーザセッションは 15 分</p> <p>根拠: (FedRAMP 高ベースライン WG)</p> <p>-----</p> <p>影響レベル 2:</p> <p>RAS ベースのセッションの場合は 30 分を超えないか、非対話型ユーザセッションの場合は 60 分を超えない</p> <p>根拠: FedRAMP v2</p> <p>-----</p>
<p>SC-12; システムと通信の保護; 暗号鍵の確立と管理:</p> <p>組織は、次に従って情報システム内で使用される必要な暗号化のための暗号鍵を管理</p> <p>[設定: 組織が定めた要件; キーの世代、流通、ストレージ、アクセスや破棄].</p> <p>参照: なし</p>	<p>SC-12</p> <p>影響レベル 4-6:</p> <p>DoDI 8520.02「公開鍵インフラストラクチャと公開鍵の有効化」と DoDI 8520.03「情報システムの識別認証」</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2:</p> <p>FedRAMP 追加要件とガイダンス:</p> <p>SC-12 ガイダンス: 連邦が承認した暗号</p>
<p>SC-12 (2) ; システムと通信の保護; 暗号鍵の確立と管理 - 強化:</p> <p>対称キー</p>	<p>SC-12 (2)</p> <p>影響レベル 4-6:</p> <p>非格付けシステムでは NIST 認証</p> <p>格付けシステムでは NSA 認証</p>

<p>組織は、以下により対称暗号鍵を生成、コントロール、配布</p> <p>[選択 :</p> <ul style="list-style-type: none">- NIST FIPS 準拠 ;- NSA 承認済み <p>]</p> <p>鍵管理技術とプロセス。</p> <p>参照 : なし</p>	<p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2 :</p> <p>NIST FIPS 準拠</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>
<p>SC-13; システムと通信の保護; 暗号の使用</p> <p>RENAMED : 暗号保護 :</p> <p>情報システムは、</p> <p>[設定 : 組織が定めた暗号利用と各用途に必要な暗号の種類]</p> <p>適用される連邦法、大統領令、指令、方針、規制、および基準に準拠</p> <p>参照 : なし</p>	<p>SC-13</p> <p>影響レベル 4-6 :</p> <p>格付情報の保護 : NSA 承認の暗号化; デジタル署名とハッシングの提供 : FIPS で検証された暗号</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2 :</p> <p>FIPS で検証済みまたは NSA で承認された暗号</p> <p>根拠 : FedRAMP v2</p> <p>-----</p>
<p>SC-15; システムと通信の保護; コラボレーティブコンピューティングデバイス :</p> <p>情報システム :</p>	<p>SC-15</p> <p>影響レベル 4-6 :</p> <p>a. 集中管理され、承認された VTC¹¹³の場所に配置された専用の VTC スイート。</p>

¹¹³ 訳注 : ビデオ遠隔会議 (VTC)

<p>a. 次の例外を除き、コラボレーティブコンピューティングデバイスのリモートアクティベーションを禁止</p> <p>[設定：組織が定めた活性化が許可される例外];</p> <p>そして</p> <p>b. 利用中であることを利用者へ明示する。</p> <p>参照：NIST Special Publication 800-28; DoD 命令 8552. 01</p>	<p>根拠：DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2：</p> <p>a. 例外なく</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>SC-17; システムと通信の保護; 公開鍵基盤の証明書:</p> <p>組織は、公開鍵証明書を発行</p> <p>[設定：組織が定めた証明書ポリシー]</p> <p>承認されたサービスプロバイダから公開鍵証明書を取得</p> <p>参 照：OMB 覚 書 08-23; NIST Special Publication 800-81.</p>	<p>SC-17</p> <p>影響レベル 4-6：</p> <p>DoDI 8520.02 「公開鍵インフラストラクチャ (PKI) と公開鍵 (PK) を有効にする」</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>
<p>SC-23 (3) ; システムと通信の保護; セッション認証 - 強化:</p> <p>ランダム化による一意のセッション識別子</p> <p>情報システムは、次によりセッションごとに固有のセッション識別子を生成</p> <p>[設定：組織が定めたランダム性要件]</p> <p>システムで生成されたセッション識別子のみを認識</p> <p>参照：NIST Special Publications 800-56, 800-57, 800-111.</p>	<p>SC-23 (3)</p> <p>[値は未設定。 CSP により設定される]</p>

<p>SC-23 (5) ; システムと通信の保護; セッション認証 - 強化: 許可された認証局</p> <p>情報システムは、次だけの利用を許可 [設定: 組織が定めた認証機関] 保護されたセッションの確立を検証</p> <p>参照: なし</p>	<p>SC-23 (5)</p> <p>影響レベル 4-6 : DoD PKI が証明局を設立</p> <p>根拠: DoD RMF TAG -----</p>
<p>SC-28; システムと通信の保護; 保管された情報の保護:</p> <p>情報システムは、次を保護 [選択 (1 つまたは複数): - 機密性; - 完全性] 次の [設定: 組織が定めた保存情報].</p> <p>参照: なし</p>	<p>SC-28</p> <p>すべての影響レベル: 機密性と完全性</p> <p>根拠: FedRAMP v2 -----</p> <p>FedRAMP 追加要件とガイダンス: SC-28. ガイダンス: 組織は、保管中の情報を保護するために暗号メカニズムを使用する機能をサポート。</p>
<p>SC-28 (1) ; システムと通信の保護; 保管された情報の保護 - 強化: 暗号保護</p> <p>情報システムは、不正な開示や改ざんを防ぐための暗号メカニズムを実装 [設定: 組織が定めた情報] 次に [設定: 組織が定めた情報システムコンポーネント].</p> <p>参照: なし</p>	<p>SC-28 (1)</p> <p>影響レベル 4-6 : SC-28 (1) 値 1 で定義されたデータを格納する情報システムコンポーネント。</p> <p>根拠: DoD RMF TAG -----</p>

<p>SI-1; システムと情報の完全性; システムと情報の完全性の方針と手順:</p> <p>組織:</p> <p>a. 開発、文書化、配布</p> <p>[設定: 組織が定めた要員または役割]:</p> <ol style="list-style-type: none"> 1. 目的、範囲、役割、責任、管理を扱うシステムと情報の完全性ポリシー、コミットメント、組織間の調整、コンプライアンスを記述した完全性の方針—そして 2. システムと情報の完全性の方針や関連する情報の完全性コントロールの実施を促進するための手続—そして <p>b. 現状のレビューと更新:</p> <ol style="list-style-type: none"> 1. システムと情報の完全性の方針 <p>[設定: 組織が定めた頻度]; そして</p> <ol style="list-style-type: none"> 2. システムと情報の完全性の手順 <p>[設定: 組織が定めた頻度].</p> <p>参照: NIST Special Publication 800-83.</p>	<p>SI-1</p> <p>影響レベル 4-6:</p> <p>a. すべての任命された情報保証の要員</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル:</p> <p>b.1 少なくとも3年ごと</p> <p>b.2 少なくとも年に1回</p> <p>根拠: FedRAMP v2</p> <p>-----</p>
<p>SI-2; システムと情報の完全性; 欠陥の是正:</p> <p>組織:</p> <p>a. 情報システムの欠陥を特定し、報告し、是正する。</p> <p>b. 是正の有効性と欠陥の是正に伴う潜在的な副作用について、ソフトウェアとファームウェアのアップデートの検証</p> <p>c. ソフトウェアとファームウェアについて、セキュリティ関連の更新を次の期間内にインストール</p> <p>[割当: 組織が定めた期間]</p> <p>更新のリリース時点から。そして</p>	<p>SI-2</p> <p>影響レベル 4-6:</p> <p>c. (IAVM、CTO、DTM、STIG など) の承認期間内またはアップデートのリリース後30日以内に</p> <p>根拠:</p> <p>DoD RMF TAG と FedRAMP v2</p> <p>-----</p> <p>影響レベル 2:</p> <p>c. アップデートのリリースから30日以内</p>

<p>d. 組織の構成管理プロセスに欠陥の是正を組込む</p> <p>参照：なし</p>	<p>根拠：FedRAMP v2</p> <p>-----</p>
<p>SI-2 (2) ; システムと情報の完全性; 欠陥の是正 - 強化:</p> <p>自動欠陥修正ステータス</p> <p>組織は自動化されたメカニズムを適用</p> <p>[設定：組織が定めた頻度]</p> <p>欠陥の是正に関する情報システムコンポーネントの状態を決定</p> <p>参照：なし</p>	<p>SI-2 (2)</p> <p>影響レベル 4-6 :</p> <p>ホストベースの監視ソフトウェアで継続的に。毎年 CSSP (Cybersecurity Service Provider) による外部スキャン</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2 :</p> <p>少なくとも毎月</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>SI-2 (3) ; システムと情報の完全性; 欠陥の是正 - 強化:</p> <p>是正措置のため時間/修復作業のベンチマーク</p> <p>組織:</p> <p>a. 欠陥の特定から欠陥の是正までの時間を測定 - そして</p> <p>b. 以下を確立</p> <p>[設定：組織が定めたベンチマーク]</p> <p>是正措置の実施について</p> <p>参照：なし</p>	<p>SI-2 (3)</p> <p>影響レベル 4-6 :</p> <p>b. (例えば、IAVM、CTO、DTM、STIG) が指示する期間内に</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>

<p>SI-2 (6) ; システムと情報の完全性; 欠陥の是正 - 強化:</p> <p>古いバージョンのソフトウェア/ファームウェアの削除</p> <p>組織は、次を削除</p> <p>[設定: 組織が定めたソフトウェアとファームウェアコンポーネント]</p> <p>更新されたバージョンがインストールされた後で。</p> <p>参照: なし</p>	<p>SI-2 (6)</p> <p>影響レベル 4-6 :</p> <p>アップグレードまたは交換されたソフトウェアおよびファームウェアのすべてのコンポーネント</p> <p>根拠: DoD RMF TAG</p> <p>-----</p>
<p>SI-3; システムと情報の完全性; 悪質なコードからの保護:</p> <p>組織:</p> <p>a. 悪意のあるコードを検出して根絶するために、情報システムの出入り口で悪意のあるコードからの保護メカニズムを実装</p> <p>b. 組織の構成管理ポリシーおよび手順に従って新しいリリースが利用可能になるたびに、悪質なコードからの保護メカニズムを更新</p> <p>c. 悪質なコードからの保護メカニズムを次のように構成</p> <p>1. 情報システムの定期スキャンの実行</p> <p>[設定: 組織が定めた頻度]</p> <p>外部からのファイルに対するリアルタイムスキャンを次のポイントで実行</p> <p>[選択 (1 つまたは複数) ;</p> <p> - エンドポイント;</p> <p> - ネットワーク出入口ポイント</p> <p>]</p> <p>組織のセキュリティポリシーに従ってファイルがダウンロード、開かれ、または実行されたときに; そして</p>	<p>SI-3</p> <p>影響レベル 4-6 :</p> <p>c. 2. 悪意のあるコードをブロックして隔離し、すぐに (リアルタイムで) またはほぼリアルタイムで管理者にアラートを送信</p> <p>根拠: DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル:</p> <p>c. 1. 少なくとも毎週 エンドポイントを含める</p> <p>影響レベル 2 :</p> <p>c. 2. アラート管理者または定義されたセキュリティ担当者を含める</p> <p>根拠: FedRAMP v2</p> <p>-----</p>

<p>2. [選択（1 つまたは複数）：</p> <ul style="list-style-type: none"> - 悪質なコードのブロック； - 悪質なコードの隔離； - 管理者へアラートを送信； - [設定：組織が定める処理] <p>]</p> <p>悪質なコードの検出に応答して、そして</p> <p>d. 悪意のあるコードの検出と駆除の際の偽陽性の判定と、結果として情報システムの可用性に影響を与える可能性があることに言及</p> <p>参照：なし</p>	
<p>SI-3（10）；システムと情報の完全性；悪意のあるコードからの保護 - 強化：</p> <p>悪質なコードの分析</p> <p>組織：</p> <p>（a）次を実行</p> <p>[課題：組織が定めたツールと手法]</p> <p>悪質なコードの特性と挙動を分析。 —そして</p> <p>（b）悪意のあるコード分析の結果を組織のインシデント・レスポンスおよび欠陥是正プロセスに組み込む。</p> <p>参照：なし</p>	<p>SI-3（10）</p> <p>[値は未設定。 CSP により設定される]</p>
<p>SI-4；システムと情報の完全性；情報システムの監視：</p> <p>組織：</p> <p>a. 情報システムを監視して以下を検出</p> <ol style="list-style-type: none"> 1. 次に従った攻撃と潜在的な攻撃の兆候 <p>[設定：組織が定めた監視目的]；そして</p> <ol style="list-style-type: none"> 2. 無許可のローカル、ネットワーク、リモート接続。 	<p>SI-4</p> <p>影響レベル 4-6：</p> <p>a. 1. CJCSI 6510.01F 内のセンサー配置とモニター要件</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>

<p>b. 以下による情報システムの不正使用の識別 [設定：組織が定めた技術と方法];</p> <p>c. 監視デバイスの展開 (i) 組織が決定した重要情報を収集するために情報システム内で戦略的に実施。そして (ii) システム内の適切な場所で、特定のタイプのトランザクションの追跡</p> <p>d. 侵入監視ツールから得た情報を不正なアクセス、変更、削除から保護</p> <p>e. 組織の業務や資産、個人、その他の組織に対するリスクの増大、国の法執行機関の情報、インテリジェンス情報、その他の信頼できる情報に基づいて、情報システムの監視活動のレベルを高める。</p> <p>f. 適用される連邦法、大統領令、指令、方針、または規制に従って情報システム・モニタリング活動に関する法務の観点からの意見を得る。そして</p> <p>g. 情報の提供 [設定：組織が定めた情報システム監視情報]</p> <p>次へ [設定：組織が定めた要員または役割] [選択（1 つまたは複数）： - 必要に応じて; - [設定：組織が定めた頻度]].</p> <p>参照：なし</p>	<p>g. DoD ミッションオーナーのシステム/アプリケーション/情報に影響を及ぼすセキュリティの態勢や脆弱性の変化に関する情報の監視</p> <p>PA と顧客の AT0 を発行した A0、および DoD ミッションオーナーの MCD</p> <p>必要に応じて。</p> <p>根拠：CC SRG DoD プロセスとの CSP 統合のベストプラクティス -----</p>
<p>SI-4 (4) ; システムと情報の完全性; 情報システムの監視 - 強化: 着信および発信通信トラフィック</p> <p>情報システムは、インバウンドおよびアウトバウンドの通信トラフィックを監視</p>	<p>SI-4 (4)</p> <p>すべての影響レベル: 継続的に</p> <p>根拠：FedRAMP v2</p>

<p>[設定：組織が定めた頻度] 異常または許可されていない活動や状態</p> <p>参照：なし</p>	<p>-----</p>
<p>SI-4 (5) ; システムと情報の完全性; 情報システムの監視 - 強化: システム生成アラート</p> <p>情報システムのアラート</p> <p>[設定：組織が定めた要員または役割] 次の不正アクセスやその兆候が発生した場合:</p> <p>[設定：組織が定めた不正アクセスの指標]</p> <p>参照：なし</p>	<p>SI-4 (5)</p> <p>影響レベル 4-6 : 少なくとも、ISSM と ISSO</p> <p>リアルタイム侵入検知、CJCSM 6510.01B 内の権威あるソース (CTO など)、インシデントカテゴリ I、II、IV、および VII で識別される脅威が存在する場合</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>すべての影響レベル: FedRAMP 追加要件とガイダンス: インシデント・レスポンス計画に従う。</p>
<p>SI-4 (12) ; システムと情報の完全性; 情報システムの監視 - 強化: 自動アラート</p> <p>組織は、自動化されたメカニズムを使用して、以下の不適切または異常な活動をセキュリティ担当者に警告</p> <p>[設定：アラートをトリガーする組織が定めた活動].</p> <p>参照：なし</p>	<p>SI-4 (12)</p> <p>影響レベル 4-6 : 権威あるソース (CTO など) や CJCSM 6510.01B に従って脅威が特定された場合</p> <p>根拠：DoD RMF TAG</p> <p>-----</p>

<p>SI-4 (19) ; システムと情報の完全性; 情報 システムの監視 - 強化 : リスクの高い個人</p> <p>組織は、次を実施 [設定 : 組織が定めた追加の監視] 次により特定された個人 [設定 : 組織が定めた情報源] リスクのレベルが上昇</p> <p>参照 : なし</p>	<p>SI-4 (19)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>SI-4 (20) ; システムと情報の完全性; 情報 システムの監視 - 強化 : 特権ユーザ</p> <p>組織は、次を実施 [設定 : 組織が定めた追加モニタリング] 特権ユーザについて</p> <p>参照 : なし</p>	<p>SI-4 (20)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>SI-4 (22) ; システムと情報の完全性; 情報 システムの監視 - 強化 : 不正ネットワークサービス</p> <p>情報システムにおける、許可されていない、 または承認されていないネットワークサービ スの検出 [設定 : 組織が定めた認定または承認プロセ ス] そして [選択 (1 つまたは複数) : - 監査 ; - アラート [設定 : 組織が定めた要員また は役割]].</p>	<p>SI-4 (22)</p> <p>影響レベル 4-6 : 最小限でも、ISSM または ISS0、およびミ ッションオーナーの MCD へアラート</p> <p>根拠 : DoD RMF TAG (商用 CSP の調整あ り) -----</p>

<p>参照：なし</p>	
<p>SI-4 (23) ; システムと情報の完全性; 情報システムの監視 - 強化 : ホストベースのデバイス</p> <p>組織は、 [設定：組織が定めたホストベースの監視メカニズム] 次について [設定：組織が定めた情報システムコンポーネント].</p> <p>参照：NIST Special Publications 800-147、80-155</p>	<p>SI-4 (23)</p> <p>影響レベル 4-6 : ホストベースの監視ソフトウェア</p> <p>すべてのコンポーネント</p> <p>根拠：DoD RMF TAG -----</p>
<p>SI-5; システムと情報の完全性; セキュリティアラート、勧告や指示 :</p> <p>組織 :</p> <p>a. 情報システムのセキュリティ警告、勧告や指示を次から受領 [設定：組織が定める外部組織]から継続的に</p> <p>b. 必要に応じて、内部セキュリティアラート、勧告や指示を生成</p> <p>c. セキュリティアラート、勧告や指令を次の目的で配布 [選択 (1 つまたは複数) : - [設定：組織が定めた要員または役割]; - [設定：組織が定めた組織内の部門]; - [設定：組織が定めた外部組織]];</p>	<p>SI-5</p> <p>影響レベル 4-6 :</p> <p>a. 最低限、USCYBERCOM</p> <p>c. ISSO と ISSM</p> <p>c. セキュリティアラート、勧告や指令の受領者として要素が選択されていないため適用されない。</p> <p>c. 検証のため JFHQ-DoDIN。JFHQ-DoDIN はその情報を認定 CSSP へ提出する。CSSP は、すべてのミッションオーナーが情報を確実に受け取るようにする責任がある。ミッションオーナー組織は、すべての現場の</p>

<p>そして</p> <p>d. 設定した時間フレームに従って、セキュリティの指示を発効するか、問題の組織の違反の度合いを通知</p> <p>参照：なし</p>	<p>運用センター/LAN ショップへ情報を確実に提供する。</p> <p>(すなわち、コンポーネント IT システムやセキュリティ担当者)</p> <p>(ISSM、ISSO、システム管理者など)</p> <p>根拠：DoD RMF TAG</p> <p>-----</p> <p>影響レベル 2：</p> <p>a. US-CERT を含める。</p> <p>c. 構成/パッチ管理の責任を持つシステムセキュリティ担当者と管理者を含める。</p> <p>根拠：FedRAMP v2</p> <p>-----</p>
<p>SI-6；システムと情報の完全性；セキュリティ機能の検証：</p> <p>情報システム：</p> <p>a. 次の正常な運用を検証</p> <p> [設定：組織が定めたセキュリティ機能]；</p> <p>b. 次の検証を実行</p> <p> [選択（1 つまたは複数）：</p> <p> [設定：組織が定めたシステム移行状態]；</p> <p> - 適切な特権を持つユーザによるコマンドによる。</p> <p> - [設定：組織が定めた頻度]</p> <p>]；</p> <p>c. 通知</p> <p> [設定：組織が定めた要員または役割]</p> <p>失敗したセキュリティ検証テスト そして</p> <p>d. [選択（1 つまたは複数）：</p>	<p>SI-6</p> <p>すべての影響レベル：</p> <p>b. システムの起動・再起動を含め、少なくとも毎月</p> <p>c. システム管理者とセキュリティ担当者を含める。</p> <p>d. システム管理者とセキュリティ担当者への通知を含める。</p> <p>根拠：DoD RMF TAG と FedRAMP v2</p> <p>-----</p>

<ul style="list-style-type: none"> - 情報システムの停止； - 情報システムの再起動； - [設定：組織が定めた代替処置] <p>]</p> <p>異常が発見されたとき。</p> <p>参照：なし</p>	
<p>SI-7；システムと情報の完全性；情報システムの監視</p> <p>RENAMED：ソフトウェア、ファームウェアと情報の完全性：</p> <p>組織は、完全性検証ツールを使用して不正な変更を検出</p> <p>[設定：組織が定めたソフトウェア、ファームウェアと情報].</p> <p>参照：なし</p>	<p>SI-7</p>
<p>SI-7 (1)；システムと情報の完全性；情報システムの監視</p> <p>RENAMED：ソフトウェア、ファームウェア、および情報の完全性 - 強化：</p> <p>完全性の検証</p> <p>情報システムは、次の完全性を検証</p> <p>[設定：組織が定めたソフトウェア、ファームウェアと情報]</p> <p>[選択（1 つまたは複数）：</p> <ul style="list-style-type: none"> - 起動時； - [設定：組織が定めた過渡的状态またはセキュリティ関連のイベント]； - [設定：組織が定めた頻度] <p>].</p> <p>参照：なし</p>	<p>SI-7 (1)</p> <p>すべての影響レベル：</p> <p>セキュリティ関連イベントを含めるよう選択し、少なくとも毎月</p> <p>根拠：FedRAMP v2</p> <p>-----</p>

<p>SI-7 (7) ; システムと情報の完全性; ソフトウェア、ファームウェア、および情報の完全性 - 強化 :</p> <p>検出と対処の統合</p> <p>組織は、次の不正を検出</p> <p>[設定 : 組織が定めた情報システムに対するセキュリティ関連の変更]</p> <p>組織のインシデント・レスポンス機能に組み込む。</p> <p>参照 : なし</p>	<p>SI-7 (7)</p> <p>[値は未設定。 CSP により設定される]</p>
<p>SI-10; システムと情報の完全性; 入力情報の検証 :</p> <p>情報システムは、次の有効性を検証</p> <p>[設定 : 組織が定めた情報入力].</p> <p>参照 : なし</p>	<p>SI-10</p> <p>影響レベル 4-6 :</p> <p>組織によって特定されたものを除くすべての入力</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p>
<p>SI-11; システムと情報の完全性; エラー処理 :</p> <p>情報システム :</p> <p>a. 攻撃者が悪用する可能性のある情報を含まない、是正処置に必要な情報を提供するエラーメッセージを生成する。 そして</p> <p>b. エラーメッセージのみを表示</p> <p>[設定 : 組織が定めた要員または役割].</p> <p>参照 : なし</p>	<p>SI-11</p> <p>影響レベル 4-6 :</p> <p>b. ISSO、ISSM、および SCA</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p>

SI-16; システムと情報の完全性; メモリ保護: 情報システムは、 [設定: 組織が定めたセキュリティ保護手段] メモリを不正なコードの実行から保護 参照: なし	SI-16 [値は未設定。 CSP により設定される]
---	------------------------------------

表 9 は、パラメータ値を必要とした契約/SLA で対処されるセキュリティ管理策／強化：の表 3 に示されている C/CE のみの一覧を示す。これらは、ミッションオーナーと CSP に、パラメータに関連付けられた DoD 値を通知するために提供されている。表 9 において、定義されていないパラメータ値（左側の列のパラメータに対する右側の列の参照の欠落しているパラメータ）について、ミッション所有者は、C/CE を選定する際の契約/SLA の値、CSP が割り当てた値、または CSP との交渉結果の値を指定しなければならない。

注意：これらのテーブルには、FedRAMP 高ベースラインで追加された C/CE を含まない。

表 9 表 3 に示された SLA コントロール／強化のパラメータ値

AC-2 (13) ; アクセス制御; アカウント管理 - 強化 : リスクの高い個人のアカウントの無効化 組織は、重要なリスクを抱えるユーザのアカウントを無効にする [割当：組織が定めた期間] リスクの発見 参照：なし	AC-2 (13) 影響レベル 4-6 : 正式な組織の方針で特に定めがない限り 30 分 根拠：DoD RMF TAG -----
---	---

<p>AC-3 (4) ; アクセス制御; アクセス強制 - 強化 :</p> <p>自由裁量アクセス制御</p> <p>情報システムは次を強制</p> <p>[設定 : 組織が定めた自由裁量アクセス制御ポリシー]</p> <p>定義されたサブジェクトとオブジェクトに対して、情報へのアクセスを許可されたサブジェクトが次のうちの 1 つ以上を実行できることをポリシーで指定</p> <p>a. 情報を他のサブジェクトまたはオブジェクトに渡す。</p> <p>b. 特権を他のサブジェクトへ付与</p> <p>c. サブジェクト、オブジェクト、情報システム、または情報システムのコンポーネントのセキュリティ属性の変更</p> <p>d. 新しく作成または変更されたオブジェクトに関連付けるセキュリティ属性の選択 - または</p> <p>e. アクセス制御を管理する規則の変更</p> <p>参照 : なし</p>	<p>AC-3 (4)</p> <p>[値は未定義 ; CSP により設定される]</p>
<p>AC-12 (1) ; アクセス制御; セッションの終了 - 強化 :</p> <p>ユーザが開始するログアウト/メッセージ表示</p> <p>情報システム :</p> <p>a. アクセスを得るための認証が使用されるたびに、ユーザが開始した通信セッションのログアウト機能を提供</p> <p>[設定 : 組織が定めた情報資源];</p> <p>そして</p> <p>b. 認証された通信セッションの信頼できる終了を示す明示的なログアウトメッセージをユーザへ表示</p> <p>参照 : なし</p>	<p>AC-12 (1)</p> <p>影響レベル 5-6 :</p> <p>a. すべて</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p>

<p>AC-16; アクセス制御; セキュリティ属性 :</p> <p>組織 :</p> <p>a. 以下を関連付ける手段を提供</p> <p> [設定 : 組織が定めたセキュリティ属性のタイプ]</p> <p>次を持つ</p> <p> [設定 : 組織が定めたセキュリティ属性値]</p> <p>保管、処理および送信中の情報を含む。</p> <p>b. セキュリティ属性の関連付けが行われ、情報とともに保持されることを保証</p> <p>c. 許可を設定する</p> <p> [設定 : 組織が定めたセキュリティ属性]</p> <p>ために</p> <p> [設定 : 組織が定めた情報システム];</p> <p>そして</p> <p>d. 許可の決定</p> <p> [設定 : 組織が定めた値または範囲]</p> <p>確立されたセキュリティ属性のそれぞれについて、</p> <p>参照 : なし</p>	<p>AC-16</p> <p>影響レベル 4-6 :</p> <p>c. AC-16、CCIs 2256-2258 で定義されているセキュリティ属性</p> <p>c. すべての情報システム</p> <p>d. AC-16、CCIs 2259-2261 で定義された値</p> <p>根拠 : DoD RMF TAG</p> <p>-----</p>
<p>AC-16 (6) ; アクセス制御; セキュリティ属性 - 強化 :</p> <p>組織による属性関連のメンテナンス</p> <p>組織は、要員が関連付けることを許可し、以下の関連付けを維持</p> <p> [設定 : 組織が定めたセキュリティ属性]</p> <p>次について</p> <p> [課題 : 組織が定めたサブジェクトとオブジェクト]</p> <p>次に従って</p> <p> [設定 : 組織が定めたセキュリティ方針]</p> <p>参照 : なし</p>	<p>AC-16 (6)</p> <p>[値は未定義 ; CSP により設定される]</p>

<p>AU-10; 監査と説明責任; 否認防止:</p> <p>情報システムは、個人（または個人を代理するプロセス）による実行について、虚偽の否認から保護</p> <p>[設定: 組織が定めた否認防止]</p> <p>参照: なし</p>	<p>AU-10</p> <p>影響レベル 5-6:</p> <p>DoD 8520.02 および DoDI 8520.03 によって定義された対処</p> <p>根拠: DoD RMF TAG</p> <p>-----</p>
<p>IA-3 (1); 識別と認証; デバイス識別と認証 - 強化:</p> <p>暗号の双方向認証</p> <p>情報システムは、以下を認証</p> <p>[設定: 組織が定めた特定のデバイス・デバイスのタイプ]</p> <p>確立する前に</p> <p>[選択 (1 つまたは複数):</p> <ul style="list-style-type: none"> - ローカル; - リモート; - ネットワーク <p>]</p> <p>暗号ベースの双方向認証を使用した接続</p> <p>参照: なし</p>	<p>IA-3 (1)</p> <p>影響レベル 4-6:</p> <p>選択: 最小限、リモートおよびネットワーク</p> <p>DoD 補足ガイダンス: デバイスが認証されたら、最小特権の原則を使用して承認する必要がある。</p>
<p>SC-7 (11); システムと通信の保護; 境界保護 - 強化:</p> <p>着信通信トラフィックの制限</p> <p>情報システムは、以下の着信トラフィックだけを許可</p> <p>[設定: 組織が定めた認可された情報源] から</p> <p>[設定: 組織が定めた許可された宛先] へのルート</p> <p>参照: なし</p>	<p>SC-7 (11)</p> <p>影響レベル 4</p>

<p>SC-7 (14) ; システムと通信の保護; 境界保護 - 強化 : 許可されていない物理接続からの保護</p> <p>組織は、次により不正な物理的接続を保護 [設定 : 組織が定めた管理インターフェース]</p> <p>参照 : なし</p>	<p>C-7 (14)</p> <p>影響レベル 4-5 : インターネットアクセスポイント、LAN から WAN への隔離、クロスドメインソ リューション、DoD が許可した代替ゲ ートウェイなどによる。</p> <p>根拠 : DoD RMF TAG -----</p>
<p>SC-18 (3) ; システムと通信の保護; モバイル コード - 強化 : ダウンロード/実行の防止</p> <p>情報システムは、次のダウンロードと実行を防 止 [設定 : 組織が定めた容認できないモバイルコ ード]</p> <p>参照 : なし</p>	<p>SC-18 (3)</p> <p>影響レベル 5-6 :</p> <p>次のようなすべての容認できないモバ イルコード :</p> <ul style="list-style-type: none">• DoD CIO によってリスク評価を受け ておらず、リスクカテゴリに割り当て られている新興モバイルコードテクノ ロジ。• 署名のないカテゴリ 1 のモバイルコ ードやブロックまたは無効にすること ができない、カテゴリ 1 のモバイルコ ード技術 (Windows Scripting Host な ど)。• 安全なチャネル (例えば、SIPRNet、 SSL 接続、S/MIME、コードが承認された コード署名証明書で署名されている) 上で信頼できるソースから取得されて いないカテゴリ 2 のモバイルコード。 <p>根拠 : CNSS 1253</p>

	<p>補足ガイダンス：</p> <p>CSP は、CSO をサポートするインフラストラクチャを保護するために、組織の IT システムおよび CSO をサポートするインフラストラクチャにこのコントロールを適用する必要がある。</p> <p>ミッションオーナー、エンドユーザ、ネットワークの保護のため、CSP CSO は、DoD に受け入れられないと思われるモバイルコードのダウンロードを許すべきではない。</p> <p>詳細はセクション 5.16：モバイルコードを参照</p>
<p>SC-18 (4)；システムと通信の保護；モバイルコード - 強化：</p> <p>自動実行の防止</p> <p>情報システムは、次のモバイルコードの自動実行を防止する。</p> <p>[設定：組織が定めたソフトウェアアプリケーション]</p> <p>次を強制</p> <p>[設定：組織が定めたアクション]コードの実行前</p> <p>参照：NIST Special Publication 800-81</p>	<p>SC-18 (4)</p> <p>影響レベル 5-6：</p> <p>電子メール、埋め込みコードを有する文書（例えば、MS Office アプリケーション/文書）をサポートするスクリプト可能な文書/ファイル編集アプリケーションなどのソフトウェアアプリケーション。</p> <p>ユーザに許可を求めるプロンプトを発行</p> <p>根拠：CNSS 1253、民間 CSP の調整を伴う DoD RMF TAG</p>

付録E プライバシー・オーバーレイの C/CE 表と値の比較

この付属書は、FedRAMP と FedRAMP+ C/CE ベースラインに追加または修正される C/CE の表である。プライバシー・オーバーレイから与えられたパラメータ値を持つ C/CE の表が追加されている。

このセクションには、以下の表が含まれる。

- ・ 表 10- 修正または規則から要求される FedRAMP M C/CE
- ・ 表 11- 修正または規則から要求される FedRAMP+ C/CE
- ・ 表 12- FedRAMP M または FedRAMP+に含まれないプライバシー・オーバーレイ
- ・ 表 13- FedRAMP および FedRAMP+ C/CE の PII/PHI パラメータ値
- ・ 表 14- FedRAMP M または FedRAMP+に含まれない C/CE の PII/PHI パラメータ値

将来の CC SRG は、PII や PHI の取り扱いを検討中の CS0 が、PA を得るための CS0 プライバシー・オーバーレイ・ライダーに関し、どの C/CE に対しアセスメントが必要となるかについての追加の情報を含む。ミッションオーナーの責任についても言及される。

プライバシー・オーバーレイは、オーバーレイ内でどのように言及されているかを示すために、オーバーレイ内で言及された各 C/CE に関連する 1 つ以上の記号を用いる。これらの記号は次のとおりである。

- ・ プラス記号(“+”)は、管理策を選択すべきことを示す。
- ・ 2 個のダッシュ(“--”)は管理策を選択すべきでないことを示す。**
- ・ 文字“E”は、管理策の強化の存在を示す。
- ・ 文字“G”は、管理策について該当する場合には、調整のための具体的な仕立て指針を含むガイダンスがあることを示す。
- ・ 文字“V”は、このオーバーレイが管理策として、組織が定めたパラメータの値を定義することを示す。
- ・ 文字“R”は、管理策の選択に影響を与える規制／法的参照が少なくとも 1 つ存在すること、または規制が規制／法的要件を満たすのに役立つことを示す。

**注：コード“--”を含む CE は AC-2 (8) だけであり、これにはコード“R”が含まれているため、この CE は規制上の理由から選択してはならない。

表は次のページから開始する。

表 10 修正または規則から要求される FedRAMP M C/CE

C/CE	SRGType	L4	L5/6	PIIL	PIIM	PIIH	PHI
AC-01	FR.M	X	X	+GR	+GR	+GR	+ER
AC-02	FR.M	X	X	+EGVR	+EGVR	+EGVR	+EGR
AC-02(09)	FR.M	X	X	GVR	GVR	GVR	R
AC-03	FR.M	X	X	+EGR	+EGR	+EGR	+GR
AC-04	FR.M	X	X		+GR	+GR	+R
AC-05	FR.M	X	X		+GR	+GR	+GR
AC-06	FR.M	X	X		+GR	+GR	+GR
AC-06(01)	FR.M	X	X			+GR	+R
AC-06(02)	FR.M	X	X		+GR	+GR	+R
AC-06(05)	FR.M	X	X			+R	+R
AC-06(09)	FR.M	X	X		+R	+R	+R
AC-06(10)	FR.M	X	X		+R	+R	
AC-08	FR.M	X	X	GR	GR	GR	GR
AC-11	FR.M	X	X	+EVR	+EVR	+EVR	+GR
AC-14	FR.M	X	X		GR	GR	GR
AC-17	FR.M	X	X	+GR	+GR	+GR	+GR
AC-17(01)	FR.M	X	X	+GR	+GR	+GR	+R
AC-17(02)	FR.M	X	X	+R	+R	+R	+GR
AC-18(01)	FR.M	X	X	+GR	+GR	+GR	
AC-19	FR.M	X	X	+ER	+ER	+ER	+GR

AC-19(05)	FR.M	X	X	+EVR	+EVR	+EVR	+GVR
AC-20	FR.M	X	X	+EGR	+EGR	+EGR	+R
AC-20(01)	FR.M	X	X	+R	+R	+R	+R
AC-21	FR.M	X	X	+GR	+GR	+GR	+GR
AC-22	FR.M	X	X	+GR	+GR	+GR	+R
AT-01	FR.M	X	X	+GR	+GR	+GR	+R
AT-02	FR.M	X	X	+ER	+ER	+ER	+GR
AT-03	FR.M	X	X	+ER	+ER	+ER	+R
AT-04	FR.M	X	X	+GR	+GR	+GR	+R
AU-01	FR.M	X	X	+GVR	+GVR	+GVR	+R
AU-02	FR.M	X	X	+GVR	+GVR	+GVR	+GR
AU-03	FR.M	X	X	+GR	+GR	+GR	+R
AU-04	FR.M	X	X		+GR	+GR	+R
AU-06	FR.M	X	X		+GR	+GR	+R
AU-06(03)	FR.M	X	X		+R	+R	
AU-07	FR.M	X	X	+R	+R	+R	+R
AU-07(01)	FR.M	X	X		+R	+R	+R
AU-09	FR.M	X	X	+GR	+GR	+GR	+R
C/CE	SRGType	L4	L5/6	PIIL	PIIM	PIIH	PHI
AU-09(04)	FR.M	X	X		GR	GR	
AU-12	FR.M	X	X		+R	+R	+R

CA-01	FR.M	X	X	+GR	+GR	+GR	+R
CA-02	FR.M	X	X	+GR	+GR	+GR	+VR
CA-03	FR.M	X	X		+R	+R	+GVR
CA-03(03)	FR.M	X	X	+VR	+VR	+VR	+R
CA-03(05)	FR.M	X	X	+VR	+VR	+VR	+R
CA-06	FR.M	X	X	+EGR	+EGR	+EGR	+GR
CA-07	FR.M	X	X		+GR	+GR	+GR
CA-08	FR.M	X	X			+GVR	
CA-09	FR.M	X	X		+GVR	+GVR	+VR
CM-04	FR.M	X	X	+GR	+GR	+GR	+R
CP-01	FR.M	X	X	+R	+R	+R	+R
CP-02	FR.M	X	X	+R	+R	+R	+GR
CP-07	FR.M	X	X		GR	GR	GVR
CP-09	FR.M	X	X		+ER	+ER	+ER
CP-10	FR.M	X	X		+R	+R	+R
IA-02	FR.M	X	X	+R	+R	+R	+R
IA-02(11)	FR.M	X	X		+GR	+GR	
IA-04	FR.M	X	X	+ER	+ER	+ER	+GR
IA-05	FR.M	X	X		+R	+R	+GR
IA-07	FR.M	X	X	+GR	+GR	+GR	+GR
IA-08	FR.M	X	X		+R	+R	+R

IR-01	FR.M	X	X	+GVR	+GVR	+GVR	+GR
IR-02	FR.M	X	X	+GR	+GR	+GR	+GR
IR-04	FR.M	X	X	+GR	+GR	+GR	+GR
IR-05	FR.M	X	X	+GR	+GR	+GR	+R
IR-06	FR.M	X	X	+GVR	+GVR	+GVR	+R
IR-07	FR.M	X	X	+GR	+GR	+GR	+R
IR-08	FR.M	X	X	+GR	+GR	+GR	+GR
MA-01	FR.M	X	X		+ER	+ER	+GR
MA-05	FR.M	X	X	+GR	+GR	+GR	+GR
MP-01	FR.M	X	X	+VR	+VR	+VR	+VR
MP-02	FR.M	X	X	+VR	+VR	+VR	+VR
MP-03	FR.M	X	X	+GR	+GR	+GR	+GR
MP-04	FR.M	X	X	+VR	+VR	+VR	+R
MP-05	FR.M	X	X	+VR	+VR	+VR	+VR
MP-05(04)	FR.M	X	X	+R	+R	+R	+GR
MP-06	FR.M	X	X		+GVR	+GVR	+VR
C/CE	SRGType	L4	L5/6	PIIL	PIIM	PIIH	PHI
MP-07	FR.M	X	X		+GVR	+GVR	
MP-07(01)	FR.M	X	X		+R	+R	
PE-02	FR.M	X	X	+R	+R	+R	+GR
PE-03	FR.M	X	X	+R	+R	+R	+R

PE-05	FR.M	X	X	+GR	+GR	+GR	+GR
PE-17	FR.M	X	X	+GR	+GR	+GR	
PL-02	FR.M	X	X	+EGR	+EGR	+EGR	+R
PL-04	FR.M	X	X	+EGR	+EGR	+EGR	
PL-08	FR.M	X	X	+GR	+GR	+GR	
PS-01	FR.M	X	X	+ER	+ER	+ER	+R
PS-02	FR.M	X	X	+ER	+ER	+ER	+GR
PS-03	FR.M	X	X	+ER	+ER	+ER	+GR
PS-03(03)	FR.M	X	X	+GVR	+GVR	+GVR	+GR
PS-04	FR.M	X	X	+GR	+GR	+GR	+GR
PS-05	FR.M	X	X	+ER	+ER	+ER	+GR
PS-06	FR.M	X	X	+GR	+GR	+GR	+R
PS-07	FR.M	X	X	+GR	+GR	+GR	+R
PS-08	FR.M	X	X	+EGR	+EGR	+EGR	+R
RA-01	FR.M	X	X	+EGR	+EGR	+EGR	+R
RA-02	FR.M	X	X	+ER	+ER	+ER	+R
RA-03	FR.M	X	X	+EGVR	+EGVR	+EGVR	+GVR
SA-02	FR.M	X	X	+ER	+ER	+ER	
SA-03	FR.M	X	X	+GR	+GR	+GR	
SA-04	FR.M	X	X	+EGR	+EGR	+EGR	+ER
SA-08	FR.M	X	X	+GR	+GR	+GR	

SA-09(05)	FR.M	X	X	+EGR	+EGR	+EGR	
SA-11	FR.M	X	X		+EGR	+EGR	
SC-02	FR.M	X	X		+ER	+ER	+ER
SC-04	FR.M	X	X	+GR	+GR	+GR	+R
SC-08	FR.M	X	X	+GVR	+GVR	+GVR	+VR
SC-08(01)	FR.M	X	X	+EVR	+EVR	+EVR	+GR
SC-12	FR.M	X	X	+VR	+VR	+VR	+GR
SC-13	FR.M	X	X	+VR	+VR	+VR	+GR
SC-28	FR.M	X	X	+GVR	+GVR	+GVR	+R
SC-28(01)	FR.M	X	X	+EGR	+EGR	+EGR	+GR
SI-01	FR.M	X	X	+R	+R	+R	+R
SI-04	FR.M	X	X	+GR	+GR	+GR	+R
SI-07	FR.M	X	X	+VR	+VR	+VR	+VR
SI-10	FR.M	X	X		+VR	+VR	
C/CE	SRGType	L4	L5/6	PIIL	PIIM	PIIH	PHI
SI-11	FR.M	X	X	+VR	+VR	+VR	+VR
SI-12	FR.M	X	X	+EGR	+EGR	+EGR	+EGR

表 11 修正または規則から要求される FedRAMP+ C/CE

C/CE	SRGType	L4	L5/6	PIIL	PIIM	PIIH	PHI
AC-06(07)	FR+	X	X	+VR	+VR	+VR	+VR
AC-23	FR+	X	X	EGR	EGR	EGR	
AU-04(01)	FR+	X	X		GR	GR	R
AU-06(10)	FR+	X	X		+GR	+GR	
CM-03(06)	FR+	X	X	+GVR	+GVR	+GVR	+GVR
CM-04(01)	FR+	X	X		+GR	+GR	
MA-04(06)	FR+	X	X	+R	+R	+R	+R
SC-08(02)	FR+		X		+GVR	+GVR	

表 12 FedRAMP M または FedRAMP+に含まれない C/CE プライバシー・オーバーレイ

C/CE	SRGType	L4	L5/6	PIIL	PIIM	PIIH	PHI
AC-02(13)	SLA	X	X	+R	+R	+R	+R
AC-03(09)	+	X	X		+EVR	+EVR	+R
AC-04(08)	+	X	X			+VR	
AC-04(15)	+	X	X		+GR	+GR	+R
AC-04(17)	+	X	X		+GVR	+GVR	
AC-04(18)	+	X	X		+GR	+GR	+R
AC-16	SLA	X	X	+GVR	+GVR	+GVR	+GVR
AC-16(03)	+	X	X	+GVR	+GVR	+GVR	+GVR

AC-20(03)	1253	X	X	+EGV R	+EGVR	+EGVR	
AU-07(02)	+	X	X		+R	+R	+R
AU-09(03)	+	X	X		+GR	+GR	+GR
AU-10	SLA/1253	X	X		+GR	+GR	+R
AU-10(01)	+	X	X		+GR	+GR	+R
AU-12(03)	1253	X	X		+VR	+VR	+VR
CA-09(01)	+	X	X		+GR	+GR	+R
CM-04(02)	+	X	X		+R	+R	+R
IA-02(06)	+	X	X		+GR	+GR	
IA-02(07)	+	X	X		+GR	+GR	
IA-04(03)	+	X	X		+GR	+GR	
IR-10	1253	X	X	+GR	+GR	+GR	
MP-06(01)	+	X	X	+GR	+GR	+GR	+GR
MP-06(08)	+	X	X		+GR	+GR	
MP-08(03)	+	X	X		+VR	+VR	+GVR
PE-18	+	X	X			+GR	+GR
PM-01	+	X	X	+GR	+GR	+GR	+R
PM-02	+	X	X	GR	GR	GR	+ER
PM-03	+	X	X	+R	+R	+R	
PM-05	+	X	X	+GR	+GR	+GR	+GR

PM-07	+	X	X	+GR	+GR	+GR	+R
PM-09	+	X	X	+ER	+ER	+ER	+ER
PM-10	+	X	X	+EGR	+EGR	+EGR	+ER
PM-11	+	X	X	+EGR	+EGR	+EGR	+R
PM-12	+	X	X	+ER	+ER	+ER	
PM-14	+	X	X	+EGR	+EGR	+EGR	
PM-15	+	X	X	+EGR	+EGR	+EGR	
PR;AP-01	+	X	X	+GR	+GR	+GR	
PR;AP-02	+	X	X	+GR	+GR	+GR	
C/CE	SRGType	L4	L5/6	PIIL	PIIM	PIIH	PHI
PR;AR-01	+	X	X	+EGR	+EGR	+EGR	+GR
PR;AR-02	+	X	X	+GR	+GR	+GR	+R
PR;AR-03	+	X	X	+ER	+ER	+ER	+ER
PR;AR-04	+	X	X	+GVR	+GVR	+GVR	+R
PR;AR-05	+	X	X	+EGR	+EGR	+EGR	+R
PR;AR-06	+	X	X	+R	+R	+R	+GR
PR;AR-07	+	X	X	+GR	+GR	+GR	+R
PR;AR-08	+	X	X	+R	+R	+R	+GR
PR;DI-01	+	X	X	+GR	+GR	+GR	
PR;DI-01(01)	+	X	X		+GR	+GR	
PR;DI-01(02)	+	X	X		+VR	+VR	

PR;DM-01	+	X	X	+GR	+GR	+GR	+R
PR;DM-02	+	X	X	+VR	+VR	+VR	+VR
PR;DM-03	+	X	X	+GR	+GR	+GR	+GR
PR;DM-03(01)	+	X	X	GR	GR	GR	+GR
PR;IP-01	+	X	X	+GR	+GR	+GR	+GR
PR;IP-02	+	X	X	+GR	+GR	+GR	+ER
PR;IP-03	+	X	X	+GR	+GR	+GR	+R
PR;IP-04	+	X	X	+R	+R	+R	+R
PR;IP-04(01)	+	X	X	GR	GR	GR	+R
PR;SE-01	+	X	X	+GR	+GR	+GR	+R
PR;SE-02	+	X	X	+GR	+GR	+GR	+R
PR;TR-01	+	X	X	+GR	+GR	+GR	+GR
PR;TR-02	+	X	X	+GR	+GR	+GR	
PR;TR-02(01)	+	X	X	+GR	+GR	+GR	
PR;TR-03	+	X	X	+R	+R	+R	
PR;UL-01	+	X	X	+EGR	+EGR	+EGR	+R
PR;UL-02	+	X	X	+EGR	+EGR	+EGR	+GR
SA-11(05)	+	X	X			+ER	
SA-15(09)	1253	X	X		+EGR	+EGR	
SA-17	+	X	X	+EGR	+EGR	+EGR	

SA-21	+	X	X	+GVR	+GVR	+GVR	+GR
SC-08(02)	1253	X			+GVR	+GVR	
SI-07(06)	+	X	X	+ER	+ER	+ER	+GR

表 13 FedRAMP と FedRAMP+ C/CE の PII/PHI パラメータ値

注：この表は PII/PHI が関連する場合、表 8 と表 9 のパラメータ値を変更するかもしれない。

<p>AC-2 アクセス制御；アカウント管理</p> <p>組織：</p> <p>a. 組織のミッション／任務機能をサポートする情報システムのアカウントのタイプを識別して選択：</p> <p> [割当：組織が定義した情報システムのアカウントタイプ]；</p> <p>b. 情報システムのアカウントへアカウント管理者を指定；</p> <p>c. グループと役割のメンバーシップの条件を決める；</p> <p>d. 各アカウントに対し、グループ、役割メンバーシップとアクセス許可（すなわち特権）その他の属性について、情報システムの許可されたユーザを指定；</p> <p>e. 次の許諾が必要；</p> <p> [割当：組織が指定した要員または役職]</p> <p>情報システムのアカウント作成要求に対し；</p> <p> [割当：組織が指定した要員または役職]</p> <p>情報システムのアカウント作成要求について；</p> <p>f. 次に従って、情報システムのアカウントを作成、有効化、修正、無効化、および削除</p> <p> [割当：組織が定めた手順または条件]；</p> <p>g. 情報システムのアカウントの利用を監視</p> <p>h. アカウント管理者へ通知：</p> <p> 1. アカウントが不要となった。</p> <p> 2. ユーザの利用終了または異動；および</p> <p> 3. 情報システムの利用または need-to-know の変化；</p> <p>i. 次に基準に情報システムのアクセスを承認：</p> <p> 1. 有効なアクセス許可；</p> <p> 2. 対象システムの使用；および</p>	<p>低と中度の PII 機密性影響度レベルのパラメータ値：</p> <p>f. 各利用者に対する年毎のプライバシートレーニングが必要であり、そうでなければアカウントが無効化される。</p>
---	---

<p>3. 組織または関連したミッション／ビジネス部門からの要請に基づく、その他の属性；</p> <p>j. アカウント管理の要件に対する準拠のレビュー</p> <p>[割当：組織が定めた頻度]；そして</p> <p>k. 個人がグループから削除されたときに、共有／グループアカウントの資格情報を再発行するプロセス（展開されている場合）の確立</p> <p>参照：なし</p>	<p>j. 少なくとも年毎</p> <p>出典 CNSSI 1253 プライバシー・オーバーレイ</p>
<p>AC-2 (9)；アクセス制御；アカウント管理—強化： 共有グループ/アカウントの使用に関する制限</p> <p>組織は、次の場合にのみ共有/グループアカウントの使用を許可</p> <p>[割当：組織が定めた共有／グループアカウントの条件確立]</p> <p>参照：なし</p>	<p>低、中および高 PII 機密性の影響レベルのパラメータ値：</p> <p>…ユーザクティビティをアカウントに一意的に帰属させるための要件……</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>
<p>AC-6 (7)；アクセス制御；最小権限—強化 ユーザ権限のレビュー</p> <p>組織： (a) レビュー [割当：組織が定めた頻度] 次へ指定した権限 [割当：組織が定めた役割またはユーザのクラス]</p> <p>各権限の必要性を検証；そして</p> <p>(b) 組織のミッション／ビジネスニーズを正しく反映するために、必要に応じて権限を再割り当てまたは削除する。</p> <p>参照：なし</p>	<p>低、中の PII 機密性影響レベルの値</p> <p>(a) 少なくとも毎年</p> <p>低や中程度の機密性影響レベル PII にアクセスする個人……</p> <p>PHI パラメータ値</p> <p>(a) 少なくとも四半期ごと…</p> <p>……特権アカウントにアクセスできる個人…</p> <p>AND</p> <p>(a) 少なくとも毎年…</p> <p>…PHI にアクセスできる個人……</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>

<p>AC-11;アクセス制御 ;セッションロック : 情報システム :</p> <p>a. 次の経過後、セッションロックを開始することにより、システムへのさらなるアクセスを防止する。</p> <p>[割当 : 組織が定めた時間]</p> <p>非アクティブであるか、またはユーザからの要求を受信 ;そして</p> <p>b. 確立された識別および認証手順を使用してユーザがアクセスを再確立するまで、セッションロックを保持する。 .</p> <p>参考 : OMB 覚書 06-16</p>	<p>低、中および高の PII 機密性影響レベルの値</p> <p>(a)少なくとも毎年</p> <p>a. 30 分以内…</p> <p>出典 : CNSSI 1253 プライバシー・オーバーレイ</p>
<p>AC-19 (5);アクセス制御 ;モバイルデバイスのアクセスコントロール ;強化</p> <p>フルデバイス / コンテナベースの暗号化</p> <p>組織は次を実行 [選択:</p> <ul style="list-style-type: none">- フルデバイス暗号化;- コンテナ暗号化 <p>]</p> <p>情報の機密性と完全性を保護するため</p> <p>[割当: 組織が定めたモバイルデバイス].</p> <p>参照 : なし</p>	<p>低、中および高の PII 機密性影響レベルの値</p> <p>…組織によって PII のアクセスが許可されたモバイルデバイスのフルデバイス暗号化またはコンテナ暗号化</p> <p>PHI パラメータ値 : …組織によって PII のアクセスが許可されたモバイルデバイスのフルデバイス暗号化またはコンテナ暗号化…</p> <p>出典 : CNSSI 1253 プライバシー・オーバーレイ</p>

<p>AU-1; 監査と説明責任 ; 監査と説明責任の方針と手順 :</p> <p>組織 :</p> <p>a. 開発、文書化し次へ配布する。</p> <p>[割当:組織が定めた要員または役割]:</p> <p>1. 目的、範囲、役割、責任、管理コミットメント、組織間の調整、コンプライアンスに対応する監査および説明責任ポリシー; そして</p> <p>2. 監査、説明責任のポリシー、関連する監査および説明責任管理の実施を促進する手順。;</p> <p>そして</p> <p>b. 現在のレビューと更新:</p> <p>1. 監査および説明責任ポリシー</p> <p>[割当:組織が定めた頻度];</p> <p>そして</p> <p>2. 監査と説明責任の手順</p> <p>[割当:組織が定めた頻度].</p> <p>参考:NIST Special Publications 800-12、800-100.</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>b. 1. 少なくとも毎年以外組織的方针に従って...</p> <p>出典:CNSSI 1253 プライバシー・オーバーレイ</p>
<p>AU-2;監査と説明責任 ; 監査対象のイベント</p> <p>組織 :</p> <p>a. 情報システムが次のイベントを監査できるかどうかを決定:</p> <p>[割当:組織が定義した監査対象のイベント];</p> <p>b. 監査関連情報を必要とする他の組織とセキュリティ監査機能を調整し、相互サポートを強化し、監査対象イベントの選択を導く;</p> <p>c. 監査対象のイベントがセキュリティインシデントの事後調査をサポートするのに十分であると考えられる理由についての根拠を提供する; そして</p> <p>d. 情報システム内で以下のイベントが監査されることを決定する:</p> <p>[割当:個々の識別されたイベントの監査について、組織が定めた監査対象のイベント(AU-2aで定義された監査対象事象のサブセット)と頻度(または必要な状況)].</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>a. PII を含む情報システムへのログイン試行の失敗や失敗を含むシステムアクセスの監視... データベースまたはデータ・リポジトリから PII を含む抽出を作成、読取り、書込み、変更、および/または削除しようとする試みの成功および失敗...</p> <p>...PII への特権アクティビティまたはシステム・レベル・アクセス...</p> <p>...異なるワークステーションからの同時ログオン...</p> <p>...すべてのプログラム、例えば、実行可能ファイル、開始</p>

<p>参考: NIST Special Publication 800-92; Web: CSRC.NIST.GOV/PCIG/CIG.HTML, IDMANAGEMENT.GOV</p>	<p>d. PII を含む情報システムへのログイン試行の失敗や失敗を含むシステムアクセスの監視… …データベースまたはデータ・リポジトリから PII を含む抽出を作成、読取り、書込み、変更、および/または削除しようとする試みの成功および失敗…</p> <p>…PII への特権アクティビティまたはシステム・レベル・アクセス…</p> <p>…異なるワークステーションからの同時ログオン…</p> <p>…すべてのプログラム、例えば、実行可能ファイル、開始…</p> <p>出典: CNSSI 1253 プライバシー・オーバーレイ</p>
<p>CA-3 (3); セキュリティアセスメントと認証; システム相互接続—強化</p> <p>格付けなしの非国家セキュリティシステムの接続</p> <p>組織は次について、直接接続を禁止 [割当: 組織が定めた格付けなし、非国家セキュリティシステム]</p> <p>次の仕組みナシで外部ネットワークへ [割当: 組織が定めた境界防護デバイス].</p> <p>参考: なし.</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>… PII を含むシステム…</p> <p>…システムへの不正アクセスを防止するために承認されたファイアウォールまたは他のネットワーク境界保護デバイス…</p> <p>出典: CNSSI 1253 プライバシー・オーバーレイ</p>
<p>CA-3 (5); セキュリティアセスメントと認証; システムの相互接続—強化</p> <p>外部システムとの接続制限</p> <p>組織は次を実施 [選択: - すべて許可,</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>… 例外として許可…</p> <p>… PII を含む情報システム…</p>

<p> - 例外として拒否; - すべて拒否, - 例外として許可] 許可のポリシー [割当: 組織が定めた情報システム] 外部の情報システムについて 参考: なし. </p>	<p> 出典: CNSSI 1253 プライ バシー・オーバーレイ </p>
<p> CA-8; セキュリティアセスメントと認証; 侵入テスト: 組織は次により侵入テストを実行 [割当: 組織が定めた頻度] 対象 [割当: 組織が定めた情報システムまたはシステムのコンポーネント]. 参考: なし. </p>	<p> 高い PII 機密性影響レベル パラメータ値: ...情報システムの承認に 先立ち、定期的に情報システム への重要な変更が発生した場合... ...高 PII 機密性影響レベル で PII を含む情報システム... 出典: CNSSI 1253 プライ バシー・オーバーレイ </p>
<p> CA-9; セキュリティアセスメントと認証; 内部システム接続 組織: a. 次により、内部接続を許可 [割当: 組織が定めた情報システム、コンポーネントまたはコンポーネント・クラス] 情報システムに対し; そして b. 各内部接続、インタフェース特性、セキュリティ要件、および伝達される情報の性質に関する文書化. 参考: なし. </p>	<p> 中、高 PII 機密性影響レベル パラメータ値: ... PII を含む情報システム PHI パラメータ値: ... PHI を含む情報システム I... 出典: CNSSI 1253 プライ バシー・オーバーレイ </p>

<p>IR-6; インシデント・レスポンス; インシデントレポート</p> <p>組織:</p> <p>a. 職員は、疑わしいセキュリティインシデントを組織内のインシデントレスポンス部署へ報告する必要がある。</p> <p>[割当: 組織が定めた機関];</p> <p>そして</p> <p>b. セキュリティインシデント情報を次へ報告</p> <p>[割当: 組織が定めた当局].</p> <p>参考: NIST Special Publication 800-61: Web: WWW.US-CERT.GOV.</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>a. PII を含むインシデントの検出または検出後、可能な限り短時間で、ただし 1 時間を超えないこと...</p> <p>b. インシデントに PII が関与する場合は、プライバシー侵害対応チームと適切なインシデントレスポンスセンター (US-CERT または IC SCC など) の両方...</p> <p>出典: CNSSI 1253 プライバシー・オーバーレイ</p>
<p>MP-1; 媒体保護; 媒体の保護ポリシーと手順</p> <p>組織:</p> <p>a. 開発、文書化して次へ配布</p> <p>[割当: 組織が定めた要員または役割]:</p> <p>1. 目的、範囲、役割、責任、管理コミットメント、組織間の調整、コンプライアンスに対応する媒体保護ポリシー; そして</p> <p>2. 媒体保護ポリシーおよび関連媒体保護制御の実施を促進する手順;</p> <p>そして</p> <p>b. 現在のレビューと更新:</p> <p>1. 媒体保護ポリシー</p> <p>[割当: 組織が定めた頻度]; そして</p> <p>2. 媒体保護手順</p> <p>[割当: 組織が定めた頻度].</p> <p>参考: NIST Special Publications 800-12、800-100.</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>a. PII への潜在的なアクセス権を持つ従業員および請負業者.....</p> <p>PHI パラメータ値:</p> <p>a. PHI へのアクセスが可能な従業員および請負業者...</p> <p>出典: CNSSI 1253 プライバシー・オーバーレイ ...</p>

<p>MP-2; 媒体保護; 媒体のアクセス:</p> <p>組織は次のアクセスを制限 [割当: 組織が定めたタイプのデジタル、非デジタル媒体]</p> <p>次に対して</p> <p>[割当: 組織が定めた要員または役割].</p> <p>参考: FIPS Publication 199; NIST Special Publication 800-111</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>…PII を含むデジタルメディアまたは非デジタルメディア……</p> <p>…正当な need-to-know を持つ認定個人…</p> <p>PHI パラメータ値:</p> <p>…PHI を含むデジタルメディアまたは非デジタルメディア……</p> <p>…正当な need-to-know を持つ認定個人…</p>
<p>MP-4; 媒体の保護; 媒体の保管:</p> <p>組織:</p> <p>a. 物理的な管理策と安全な保管</p> <p>[割当: 組織が定めたタイプのデジタルまたは非デジタル媒体]</p> <p>次の区域内</p> <p>[割当: 組織が定めた管理区域];</p> <p>そして</p> <p>b. 承認された機器、技術、手順を使用してメディアが破壊またはサニタイズされるまで、情報システム・メディアの保護を行う。.</p> <p>参考: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-11</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>a. PII を格納した可搬媒体……</p> <p>…安全が確保された区域またはロックされたコンテナ……</p> <p>出典: CNSSI 1253 プライバシー・オーバーレイ</p>
<p>MP-5; 媒体保護; 媒体の輸送:</p> <p>組織:</p> <p>a. 保護と管理策</p> <p>[割当: 組織が定めたタイプの情報システム媒体]</p> <p>管理区域外での輸送中に</p> <p>[割当: 組織が定めたセキュリティ保護措置];</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>a. PII を格納した媒体……</p> <p>…NSA 承認または FIPS 検証済みの暗号化…</p> <p>PHI パラメータ値::</p>

<p>b. 管理区域外の輸送中に情報システム媒体の説明責任を維持する；</p> <p>c. 情報システム媒体の輸送に関連する活動を文書化；そして</p> <p>d. 情報システム媒体の輸送に関連する活動を許可された要員に制限する。</p> <p>参考：FIPS Publication 199；NIST Special Publication 800-60.</p>	<p>a. PHI を格納したデジタル媒体……</p> <p>…NSA 承認または FIPS 検証済みの暗号化…</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>
<p>MP-6；媒体保護；媒体のサニタイズ：</p> <p>組織：</p> <p>a. サニタイズ</p> <p>[割当：組織が定めた情報システム媒体]</p> <p>処分の前に、組織の管理から外す、または再利用のために外す</p> <p>[割当：組織が定めたサニタイズ技術と手順]</p> <p>適用される連邦および組織の基準および方針に従って；そして</p> <p>b. セキュリティカテゴリまたは情報の分類に見合った強度と完全性を備えたサニタイズ・メカニズムを採用。</p> <p>参考：FIPS Publication 199；NIST Special Publications 800-60, 800-88；Web： www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.</p>	<p>中および高 PII 機密性影響レベルパラメータ値：</p> <p>a. PII を格納したデジタル媒体……</p> <p>…NSA の承認または FIPS で検証されたメディアサニタイズ手法または手順…</p> <p>PHI パラメータ値：</p> <p>a. PHI を格納したデジタル媒体……</p> <p>…NSA の承認または FIPS で検証されたメディアサニタイズ手法または手順…</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>
<p>MP-7；媒体保護；媒体の使用：</p> <p>組織</p> <p>[選択：</p> <p>—制限；</p> <p>—禁止</p> <p>] .</p> <p>次の使用</p> <p>[割当：組織が定めたタイプの情報システム媒体]</p> <p>次を対象に</p>	<p>中および高 PII 機密性影響レベルパラメータ値：</p> <p>… 制限…</p> <p>…ポータブルストレージおよびモバイルデバイス…</p> <p>… PII を含む情報システムおよびネットワーク，</p> <p>次の管理策なしで</p> <p>…デバイスの所有権、メディアのサニタイズと暗号化の管理策…</p>

<p>[割当：組織が定めた情報システムまたはコンポーネント]</p> <p>使って</p> <p>[割当：組織が定めたセキュリティの保護措置].</p> <p>参考：FIPS Publication 199; NIST Special Publication 800-111.</p>	<p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>
<p>PS-3 (3); 人的セキュリティ; 要員のスクリーニング - 強化: 特別な保護措置が必要な情報</p> <p>組織は、特別な保護を必要とする情報を処理、保管、または送信する情報システムにアクセスする個人を確実にすること:</p> <p>(a) 割り当てられた公的政府の職務によって証明される有効なアクセス権限を有する; そして</p> <p>(b) 次を満たす</p> <p>[割当：組織が定めた、追加のスクリーニング基準].</p> <p>参考：なし.</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>…組織は、異なるレベルの PII へのアクセスまたは PII の使用に対するリスクと責任のレベルの増加に見合った人事スクリーニング基準を定めること…</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>
<p>RA-3; リスクアセスメント; リスクアセスメント:</p> <p>組織:</p> <p>a. 情報システムの不正アクセス、使用、開示、混乱、改変、破壊、それが処理、保管、または送信する情報からの危険性の蓋然性と規模を含むリスクの評価を実施する;</p> <p>b. 次のようにリスクアセスメントの結果を文書化</p> <p>[選択:</p> <ul style="list-style-type: none"> - セキュリティ計画; - リスクアセスメント報告; - [割当：組織が定めた文書] <p>];</p> <p>c. リスクアセスメント結果のレビュー</p> <p>[割当：組織が定めた頻度];</p> <p>d. リスクアセスメントの結果を次へ配布</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>b. PII の紛失の潜在的な影響に関連するリスクの評価は、全体的なリスクアセスメントで識別しなければならない。</p> <p>すべてのリスクアセスメントの文書には、これらの知見を反映…</p> <p>PHI パラメータ値:</p> <p>b. HIPAA リスク分析、および PHI に関連するリスクは、全体的なリスクアセスメント.</p> <p>すべてのリスクアセスメント文書は、これらの知見を反映していなければならない すべての HIPAA リスク分析書類は、作成日またはそれが最</p>

<p>[割当：組織が定めた要員または役割]；そして</p> <p>e. リスクアセスメントの更新</p> <p>[割当：組織が定めた頻度]</p> <p>または、情報システムや運用環境（新しい脅威や脆弱性の特定を含む）やシステムのセキュリティ状態に影響を与える可能性のあるその他の条件に重大な変更があった場合.</p> <p>参考：なし.</p>	<p>後に効力を生じた日から 6 年間維持する必要がある…</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>
<p>SC-8；システムと通信の保護；送信の完全性</p> <p>RENAMED：送信の機密性と完全性：</p> <p>情報システムは次を保護</p> <p>[選択（1 個以上）：</p> <ul style="list-style-type: none"> - 機密性； - 完全性 <p>]</p> <p>送信される情報について</p> <p>参考：なし.</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値：</p> <p>… 機密性と完全性…</p> <p>PHI パラメータ値：… 機密性と完全性…</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>
<p>SC-8 (1)；システムと通信の保護；送信の完全性</p> <p>RENAMED：送信の機密性と完全性 - 強化:暗号または代替となる物理的保護</p> <p>情報システムは、暗号メカニズムを実装して</p> <p>[選択(1 個以上)：</p> <ul style="list-style-type: none"> - 許可のない情報の暴露； - 情報改ざんの検知 <p>]</p> <p>別に保護が無い限り、送信の間</p> <p>[割当：組織が定めた代替の物理的安全措置].</p> <p>参考：なし.</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値：</p> <p>…PII の不正な開示を防止する…</p> <p>…そこに含まれる PII への不正アクセスや改ざんを防止するための物理的安全対策……</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>

<p>SC-8 (2); システムと通信の保護; 伝送の完全性</p> <p>RENAMED: 送信の機密性と完全性 - 強化:送信前/後の扱い</p> <p>情報システムは次を維持 [選択(1個以上):</p> <ul style="list-style-type: none">- 機密性;- 完全性 <p>]</p> <p>送信準備中と受信中の情報.</p> <p>参考: なし.</p>	<p>中および高 PII 機密性影響 レベルパラメータ値:</p> <p>... 機密性と完全性...</p> <p>出典: CNSSI 1253 プライ バシー・オーバーレイ</p>
<p>SC-12; システムと通信の保護; 暗号鍵の確立と管理:</p> <p>組織は、次により情報システム内で使用される必要な 暗号化のための暗号鍵を確立し、管理する。</p> <p>[割当: 組織が定めた鍵生成、配布、ストレージ、 アクセス、および破壊の要件].</p> <p>参考: なし.</p>	<p>低、中および高の PII 機密 性影響レベルパラメータ値:</p> <p>...NIST SP 800-55 および NIST SP 800-57 に従って、 鍵の生成、配布、保管、アク セス、および破壊の集中管理 ...</p> <p>出典: CNSSI 1253 プライ バシー・オーバーレイ</p>
<p>SC-13; システムと通信の保護; 暗号の使用</p> <p>RENAMED: 暗号による保護:</p> <p>情報システムは、次を実行 [割当: 組織が定めた、各使用に必要な暗号の使 用と暗号のタイプ]</p> <p>適用される連邦法、大統領令、指令、方針、規制、お よび基準に従って。</p> <p>参考: なし.</p>	<p>低、中および高 PII 機密性 影響レベルパラメータ値:</p> <p>通過中または保管中の PII の機密性と完全性を保証する ために、FIPS で検証済みま たは NSA で承認された暗号化 ...</p> <p>出典: CNSSI 1253 プライ バシー・オーバーレイ</p>

<p>SC-28; システムと通信の保護;保管中された情報の保護:</p> <p>情報システムの次を保護</p> <p>[選択(1個以上):</p> <ul style="list-style-type: none">- 機密性;- 完全性 <p>]</p> <p>次について</p> <p>[割当:組織が定めた保管中の情報].</p> <p>参考:なし.</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>... 機密性と完全性...</p> <p>... PII...</p> <p>出典: CNSSI 1253 プライバシー・オーバーレイ</p>
<p>SI-7; システムと情報の完全性; 情報システムの監視</p> <p>RENAMED: ソフトウェア、ファームウェア、および情報の完全性:</p> <p>組織は、整合性検証ツールを使用して、許可なしの次の改ざんを検知</p> <p>[割当:組織が定めたソフトウェア、ファームウェア、および情報].</p> <p>参考:なし.</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値: ... PII...</p> <p>PHI パラメータ値: ... PHI...</p> <p>出典: CNSSI 1253 プライバシー・オーバーレイ</p>
<p>SI-10; システムと情報の完全性; 入力情報の検証:</p> <p>情報システムは次の有効性をチェック</p> <p>[割当:組織が定めた入力情報].</p> <p>参考:なし.</p>	<p>中および高 PII の機密性影響レベルパラメータ値: ... PII...</p> <p>出典: CNSSI 1253 プライバシー・オーバーレイ</p>
<p>SI-11; システムと情報の完全性; エラー処理:</p> <p>情報システムは:</p> <p>a. 敵が悪用する可能性のある情報を明らかにすることなく、是正処置に必要な情報を提供するエラーメッセージを生成する; そして</p> <p>b. エラーメッセージを次にのみを表示する。</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>b. 職務を遂行する上で情報を必要とする認可された個人...</p> <p>PHI パラメータ値:</p>

<p>[割当：組織が定めた要員または役割].</p> <p>参考：なし.</p>	<p>b. 職務を遂行する上で情報を必要とする認可された個人…</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>
--	--

表 14 FedRAMP M や FedRAMP+ に含まれない C/CE の PII/PHI パラメータ値

<p>AC-3 (9)；アクセスコントロール；アクセス強制 - 強化:管理された開示</p> <p>情報システムは、確立されたシステム境界外へ情報を次の場合を除いて開示しない。:</p> <p>(a) 受信</p> <p>[割当：組織が定めた情報システムまたはシステムコンポーネント]</p> <p>次を確保</p> <p>[割当：組織が定めたセキュリティ安全措置];</p> <p>そして</p> <p>(b) [割当：組織が定めたセキュリティ安全措置]</p> <p>開示用に指定された情報の妥当性を検証するために使用される。</p> <p>参考：なし.</p>	<p>中および高 PII 機密性影響レベルパラメータ値：:</p> <p>(a) 組織または情報システム…</p> <p>…プライバシーとセキュリティ管理策は、受けとった PII の機密情報の機密性影響レベルに見合うものである…</p> <p>(b) … 付録 J, 管理策 UL-1 と UL-2…</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>
<p>AC-3 (10)；アクセスコントロール；アクセス強制 - 強化：アクセス制御メカニズムのオーバーライドの監査</p> <p>組織は、自動アクセス制御メカニズムの監査オーバーライドを採用</p> <p>[割当：組織が定めた条件].</p> <p>参考：なし.</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>…プライバシー法の下で PII を含む情報システムのアクセス制御メカニズムが無効になる状況…</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>

<p>AC-4 (8); アクセスコントロール; 情報フローの強制 - 強化:セキュリティ・ポリシー・フィルター</p> <p>情報システムは、次により情報フロー制御を行う。</p> <p>[割当: 組織が定めたセキュリティフィルター]</p> <p>次をフロー制御の決定の基礎として</p> <p>[割当: 組織が定めた情報フロー].</p> <p>参考: なし.</p>	<p>高い PII 機密性影響レベルパラメータ値:</p> <p>……最適なセキュリティ・ポリシー・フィルター、または選択した PII 値をフィルタリングする類似のテクノロジー……情報システムの境界またはドメインにわたる PII の不正転送の防止.</p> <p>出典: CNSSI 1253 プライバシー・オーバーレイ</p>
<p>AC-4 (17); アクセスコントロール; 情報フローの強制- 強化:ドメイン認証</p> <p>情報システムは、発信元および宛先ポイントを次によって一意に識別および認証する。</p> <p>[選択(1 個以上):</p> <ul style="list-style-type: none">- 組織,- システム,- アプリケーション,- 個人 <p>]</p> <p>情報の転送について.</p> <p>参考: なし.</p>	<p>中および高 PII 機密性影響レベルパラメータ値::</p> <p>…該当する組織、システム、アプリケーション、または個人…</p> <p>出典: CNSSI 1253 プライバシー・オーバーレイ</p>
<p>AC-16; アクセスコントロール; セキュリティ属性</p> <p>組織:</p> <p>a. 関連付ける手段を提供する。</p> <p>[割当: 組織が定めたセキュリティの属性]</p> <p>次の属性を持つ</p> <p>[割当: 組織が定めたセキュリティの属性値]</p> <p>保存中、プロセス中や伝送中の情報;</p> <p>b. セキュリティ属性の関連付けが行われ、情報とともに保持されることを保証する;</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>a. ユーザ (主体) が昨年にプライバシーの訓練を完了したことを示すセキュリティ属性… …PII を含むことが予定されている、または予定されているデータ構造の場合、セキュリティ属性が “PII を含む” [値] が “yes” または “no” …</p> <p>PHI パラメータ値:: a. PHI を含むことが予定されている、または予定されているデ</p>

<p>c. 許可を設定する</p> <p> [割当：組織が定めたセキュリティの属性]</p> <p>次を対象に</p> <p> [割当：組織が定めた情報システム];</p> <p>そして</p> <p>d. 許可を決定する</p> <p> [割当：組織が定めた値または範囲]</p> <p>確立されたセキュリティ属性のそれぞれについて.</p> <p>参考：なし.</p>	<p>ータ構造の場合、セキュリティ属性が "PHI を含む" [値]が "yes"または "no"...</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>
<p>AC-16 (3); アクセスコントロール; セキュリティ属性-強化:情報システム関係づけられた属性の維持</p> <p>情報システムは、次の関連性と完全性を維持する。</p> <p> [割当：組織が定めたセキュリティ属性]</p> <p>次を対象に</p> <p> [割当：組織が定めたサブジェクトとオブジェクト].</p> <p>参考：なし.</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>...PII へのアクセス権を持つ個人に対する「年間 PII トレーニング」のユーザ属性.....</p> <p>...適用可能な情報への "PII を含む"の情報属性...</p> <p>PHI パラメータ値::</p> <p>...適用可能な情報に" PHI を含む" の情報属性.....</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>
<p>AC-20 (3); アクセスコントロール; 外部情報システムの利用-強化:組織が所有していないシステム/コンポーネント/デバイス</p> <p>組織:</p> <p> [選択:</p> <p> -制限;</p> <p> -禁止</p> <p>]</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>...PII に対する制限...</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>

<p>組織が所有していない情報システム、システムコンポーネント、またはデバイスを使用して組織情報を処理、保存、または送信すること。</p> <p>参考：なし。</p>	
<p>AU-12 (3)； 監査と説明責任； 監査の生成 - 強化:承認された個人による変更</p> <p>情報システムは、次の能力を提供する。</p> <p>[割当：組織が定めた要員または役割]</p> <p>次に対して実行される監査を変更する。</p> <p>[割当：組織が定めた情報システム、コンポーネント]</p> <p>次に基づいて</p> <p>[割当：組織が定めた選択可能なイベント基準]</p> <p>以内に</p> <p>[割当：組織が定めた時間閾値].</p> <p>参考：なし。</p>	<p>中および高 PII 機密性影響 レベルパラメータ値：：</p> <p>…許可されたシステム管理者の限定されたサブセット…</p> <p>…PII を含む情報システム…</p> <p>…法執行機関、情報機関、その他の信頼できる情報源やセキュリティ事件に基づいてリスクが変化する…</p> <p>PHI パラメータ値：：</p> <p>…許可されたシステム管理者の限定されたサブセット…</p> <p>…PHI を含む情報システム…</p> <p>…法執行機関、情報機関、その他の信頼できる情報源やセキュリティ事件に基づいてリスクが変化する…</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>
<p>MP-8 (3)； 媒体保護； メディアのダウングレード-強化:管理された非格付け情報</p> <p>組織は、以下を含む情報システム・メディアをダウングレードする。</p> <p>[割当：組織が定めた管理された非格付け情報 (CUI)]</p> <p>適用される連邦および組織の基準および方針に従って公開される前に。</p> <p>参考：なし。</p>	<p>中および高 PII 機密性影響 レベルパラメータ値：</p> <p>… PII…</p> <p>PHI パラメータ値：</p> <p>… PHI…</p> <p>出典：CNSSI 1253 プライバシー・オーバーレイ</p>

<p>AR-4 ;プライバシー; 説明責任、監査、リスク管理- プライバシーの監視と監査:</p> <p>組織は、プライバシー管理と内部のプライバシーポ リシーを監視し、監査する</p> <p>[割当 : 組織が定めた頻度]</p> <p>効果的な導入の保証</p> <p>参考: The Privacy Act of 1974, 5 U.S.C. § 552 a; 連邦情報セキュリティ管理法 (FISMA: Federal Infor mation Security Management Act) of 2002, 44 U.S. C. § 3541; Section 208, E-Government Act of 200 2 (P.L. 107-347); OMB Memoranda 03-22, 05-08, 06 -16, 07-16; OMB Circular A-130.</p>	<p>低、中および高の PII 機密 性の影響レベルパラメータ値:</p> <p>…組織のセキュリティ管理 レビュースケジュールと並行 して……</p> <p>出典 : CNSSI 1253 プライバ シー・オーバーレイ</p>
<p>DI-1 (2); プライバシー; データ品質と整合性 - デ ータ品質-強化: PII の再検証</p> <p>組織は、個人または個人の権限を与えられた代理人 が、収集した個人情報に依然として正確であることを 再確認することを要求する。</p> <p>[割当 : 組織が定めた頻度].</p> <p>参考 : なし.</p>	<p>中および高 PII 機密性影響 レベルパラメータ値:</p> <p>…PII が正確で、適切で、タ イムリーで、完全であること を保証するのに必要な頻度 で; 組織のプライバシーオフ イスと協議してシステム所有 者が決定した個人の権利、利 益、または特権に対する決定 の影響に見合うものであるこ と…</p> <p>出典 : CNSSI 1253 プライバ シー・オーバーレイ</p>

<p>DM-2 ; プライバシー; データの最小化と保持- データの保存と廃棄:</p> <p>組織:</p> <p>a. 次の個人識別情報 (PII) の各コレクションを保持する。</p> <p>[割当 : 組織が定めた期間]</p> <p>通知で特定された目的を達成するため、または法律で要求される目的を達成するため;</p> <p>b. 保管方法にかかわらず、NARA が承認した記録保持スケジュールに従って、紛失、盗難、誤用、または不正アクセスを防止する方法で、PII を処分、破棄、消去、匿名化を行う; そして</p> <p>c. 使用</p> <p>[割当 : 組織が定めた技術または手段]</p> <p>PII (原本、コピー、およびアーカイブされたレコードを含む) の安全な削除または破棄を保証するため。</p> <p>参考: The Privacy Act of 1974, 5 U.S.C. § 552a (e) (1), (c) (2); Section 208 (e), E-Government Act of 2002 (P.L. 107-347); 44 U.S.C. Chapters 29, 31, 33; OMB Memorandum 07-16; OMB Circular A-130; NIST Special Publication 800-88.</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>a. 国立記録保管簿協会 (NARA: National Archives and Records Association) が承認した記録スケジュールとプライバシー法 SORN で指定された期間...</p> <p>c. NSA 承認または FIPS で検証された技術または方法...</p> <p>PHI パラメータ値:</p> <p>付録 F, 添付 6 のプライバシー・オーバーレイ 108 04/20/2015</p> <p>a. 作成日から最短で 6 年、またはそれが最後に効力を生じた日のいずれか遅い日...</p> <p>出典 : CNSSI 1253 プライバシー・オーバーレイ</p>
<p>SA-21; システムとサービスの取得; 開発者のスクリーニング:</p> <p>組織は次を開発者へ要求</p> <p>[割当 : 組織が定めた情報システム、コンポーネント、サービス]:</p> <p>a. 指定者が決定した適切なアクセス権限を持つ。</p> <p>[割当 : 組織が定めた政府の公式当局];</p> <p>そして</p> <p>b. 次を満たす</p> <p>[割当 : 組織が定めた追加の人員スクリーニング基準].</p> <p>参考 : なし.</p>	<p>低、中および高の PII 機密性の影響レベルパラメータ値:</p> <p>...PII を含むシステム.....</p> <p>a. 契約担当と契約担当の代表者が組織のプライバシーオフィスと相談して.....</p> <p>b. 組織は、異なるレベルの PII へのアクセスまたは PII の使用に対するリスクと責任のレベルの増加に見合った人員スクリーニング基準を定める...</p> <p>出典 : CNSSI 1253 プライバシー・オーバーレイ</p>

<p>SC-8 (2); システムと通信の保護; 送信の完全性</p> <p>RENAMED: 送信の機密性と完全性 -強化:送信前/送信後の処理</p> <p>情報システムは次を維持 [選択(1個以上):</p> <ul style="list-style-type: none">-機密性;-完全性 <p>]</p> <p>送信準備中および受信中の情報について.</p> <p>参考: なし.</p>	<p>中および高 PII 機密性影響 レベルパラメータ値:</p> <p>...機密性と完全性...</p> <p>出典: CNSSI 1253 プライバシー・オーバーレイ</p>
---	--

付録F 将来のプライバシー・オーバーレイガイダンス

ここは、プライバシー・オーバーレイ C/CE の適用性と補足ガイダンスに関する表のプレースホルダである。

クラウドコンピューティングのセキュリティについて
(平成30年度)

平成30年12月発行

非売品 禁無断転載・複製

発行：公益財団法人 防衛基盤整備協会

編集：防衛基盤研究センター刊行物等編集委員会

住所：〒160-0003 東京都新宿区四谷本塩町15番9号

電話：03-3358-8754 FAX：03-3358-8735

メール：koueki@bsk-z.or.jp

ホームページ：<https://www.bsk-z.or.jp>